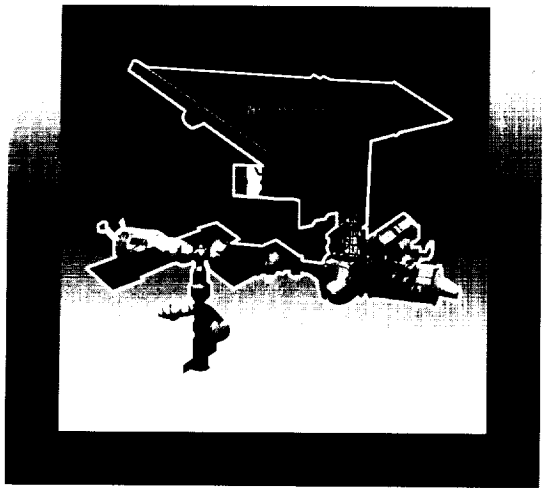
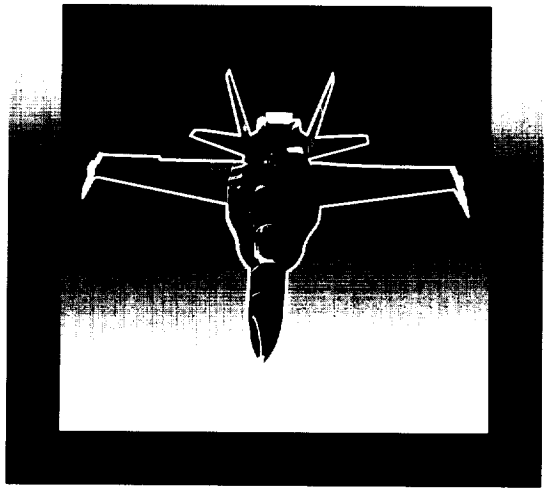
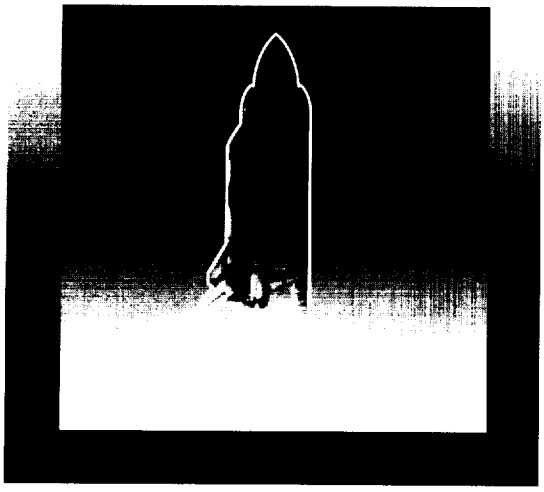
NASA-TM-110474

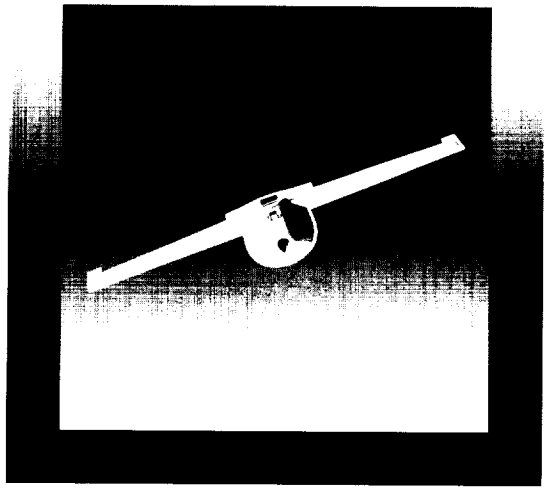
National Aeronautics and
Space Administration

AEROSPACE SAFETY ADVISORY PANEL









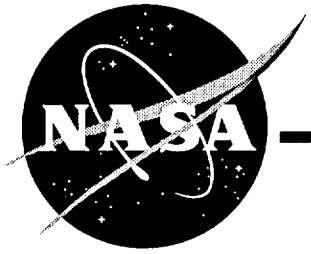
ANNUAL REPORT FEBRUARY 1996

AEROSPACE SAFETY ADVISORY PANEL

ANNUAL REPORT FEBRUARY 1996

"The Panel shall review safety studies and operations plans referred to it and shall make reports thereon, shall advise the Administrator with respect to the hazards of proposed or existing facilities and proposed operations and with respect to the adequacy of proposed or existing safety standards and shall perform such other duties as the Administrator may request."

(NASA Authorization Act of 1968, Public Law 90-67, 42 U.S.C. 2477)



Aerospace Safety Advisory Panel

Annual Report

February 1996

Aerospace Safety Advisory Panel
Code Q-1
NASA Headquarters
Washington, DC 20546

Tel: (202) 358-0914

This report is respectfully dedicated to our colleague, Walter C. Williams, who passed away on October 7, 1995. Dr. Williams was a pioneer in both aviation and space. His dedicated service to NASA and the Aerospace Safety Advisory Panel as well as his numerous technical accomplishments are legendary. We will miss his knowledge, experience and calming influence. Most of all, we will miss a friend whose advice was always insightful and constantly sought. His legacy is enormous, and we are proud to have been among its recipients.

National Aeronautic and
Space Administration

Headquarters
Washington, DC 20546-001

Reply to Attn of: Q-1

February 1996

Honorable Daniel S. Goldin
Administrator
NASA Headquarters
Washington, D.C. 20546

Dear Mr. Goldin:

The Aerospace Safety Advisory Panel is pleased to submit its annual report covering the period from February through December 1995. This was an extremely active and significant period for NASA and hence for the Panel. The restructuring of NASA and the planned consolidation of Space Shuttle operations under a Space Flight Operations Contractor (SFOC) have the potential to increase efficiency. However, they also represent substantial change and, as such, have the potential to increase risk. The Panel is confident that your strong advocacy of safety above schedule and cost will go a long way towards controlling any such increase. Restructuring the Space Shuttle Program can be accomplished while maintaining safe operations, provided it is approached cautiously and based on the extensive lessons learned from past safe Space Shuttle operations.

The Panel's frequent visits to Kennedy Space Center (KSC) have indicated that the commitment of Space Shuttle personnel to "Safety First" appears intact. This attitude prevails throughout all KSC personnel, both contractor and NASA. There are indications that distractions are up and morale may be suffering, but the professionalism of the employees and their loyalty to the Space Shuttle Program should help ensure continued safe operations.

The Panel has created three task teams to evaluate and advise NASA before, during, and after the restructuring process. One team is reviewing the operations at KSC and taking the "pulse" of the work force. The second team is assessing the potential safety impacts of NASA restructuring and the transition to the SFOC. The third team is looking at the capability of the Space Shuttle to support the manifest required to assemble and ultimately operate the International Space Station.

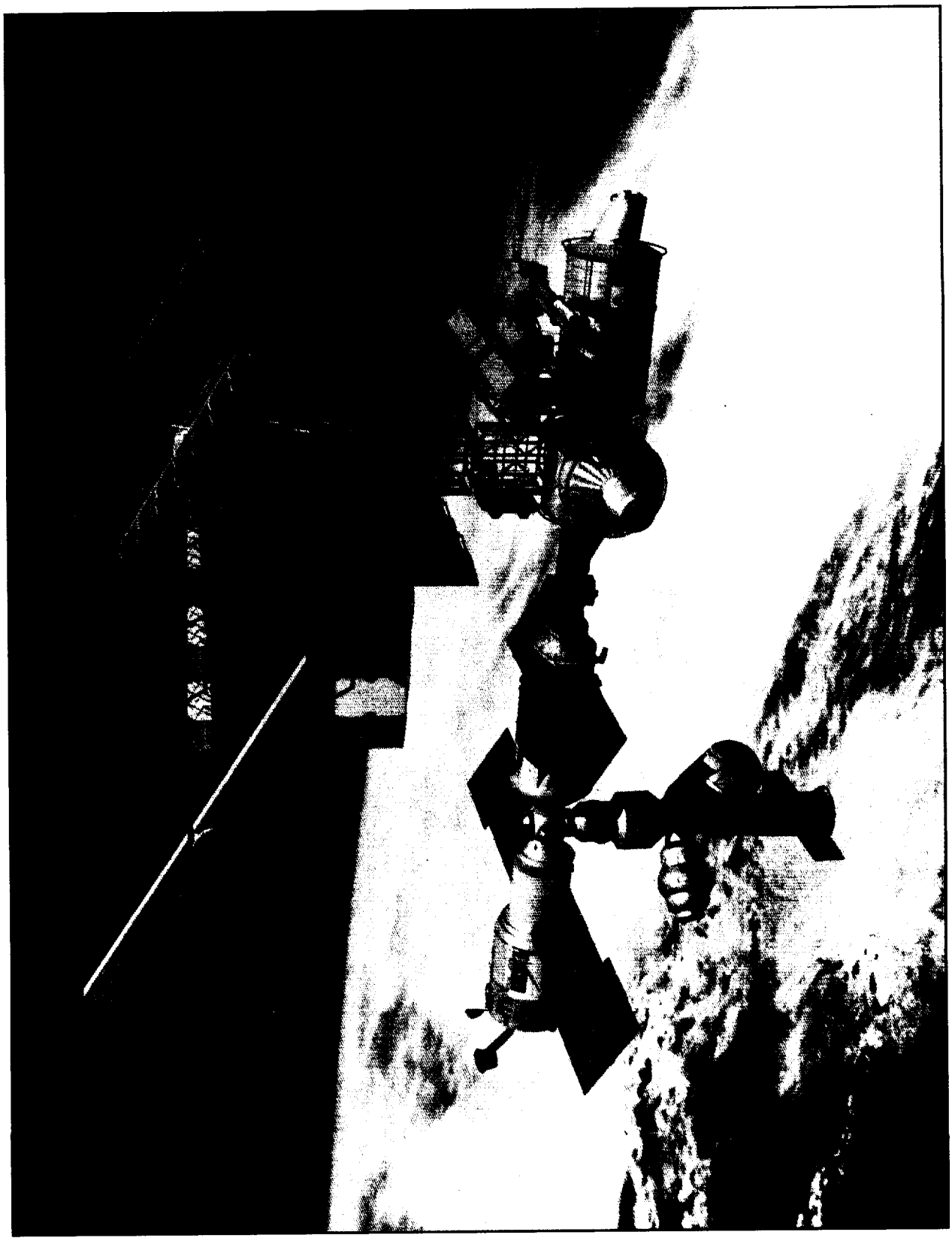
The Aerospace Safety Advisory Panel appreciates the extensive cooperation and assistance received from NASA and contractor personnel throughout the past year. NASA's timely response to Section II, "Findings and Recommendations," will greatly expedite the process of evaluation and advice.

Very truly yours,

Paul M. Johnstone
Chairman
Aerospace Safety Advisory Panel

TABLE OF CONTENTS

I. INTRODUCTION



I. INTRODUCTION

The Aerospace Safety Advisory Panel (ASAP) has traditionally attempted to canvas the full range of NASA's human spaceflight and aeronautics programs during each year's activities. Particular emphasis is then placed on those activities which are viewed as having the greatest potential for safety problems. The past year was no exception. For example, the Panel monitored Space Shuttle launch activities and was gratified by the successful missions. These included three visits to and two dockings with the Russian Mir Space Station which were accomplished with only minor anomalies. NASA's accomplishments were even more impressive in light of the organizational changes which were underway for much of the year.

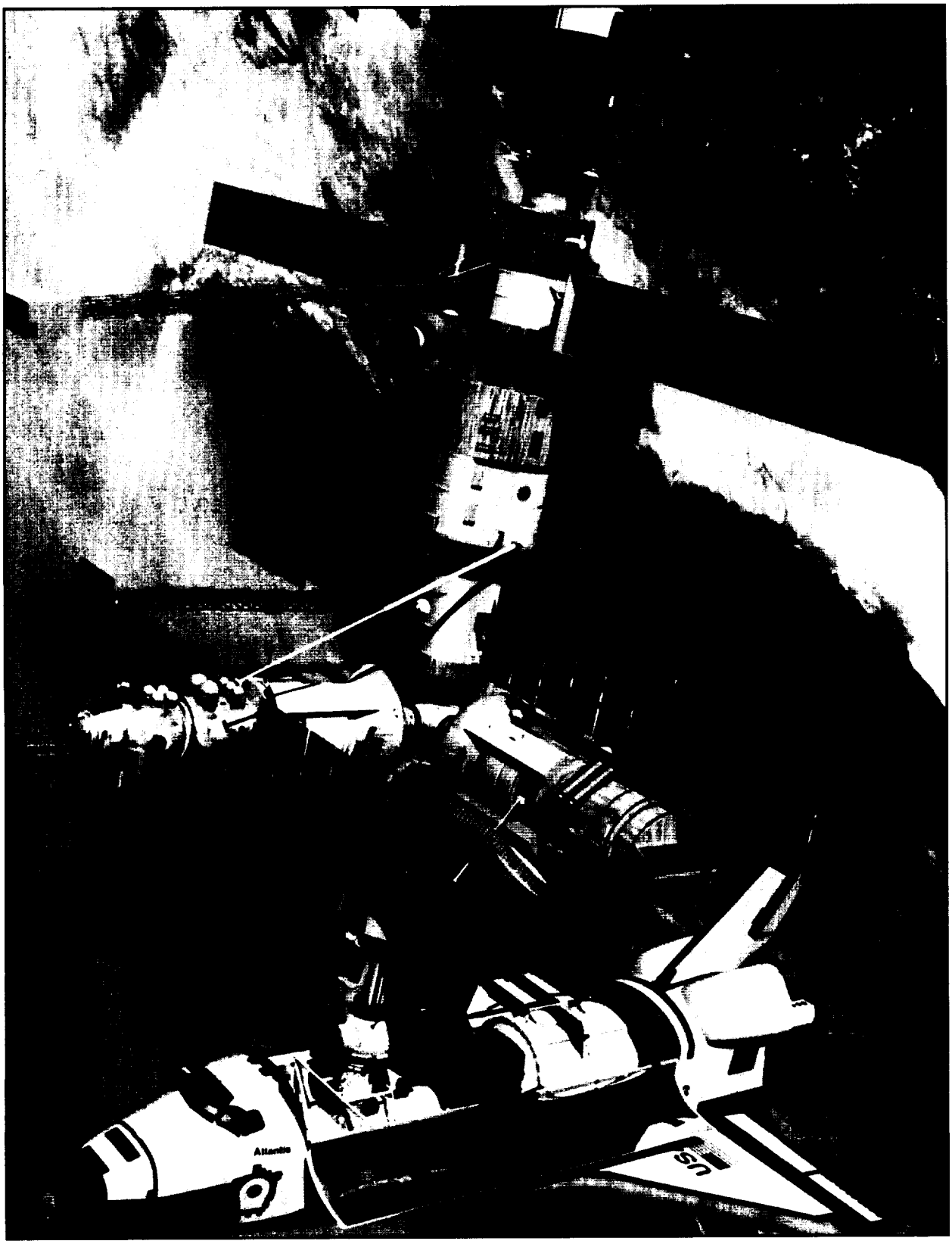
In addition to the Panel's normal oversight activities, several special investigations were conducted including one on the Phase II Space Shuttle Main Engine Turbopumps and another on the state of morale at the Kennedy Space Center. Reports on these activities were delivered to the Administrator and are not included as part of this Annual Report. The Panel also provided direct feedback to NASA Centers and contractors.

The Panel is addressing the potential for safety problems due to organizational changes by increasing its scrutiny of Space Shuttle operations and planning. Three special task teams have been formed to examine operations, transition plans and the pressures imposed by the International Space Station (ISS) flight manifest. These teams will intensify their efforts in the coming year.

The past year was also one of transition for the Panel. We mourn the passing of Dr. Walter C. Williams who was a consultant to the Panel. Paul M. Johnstone succeeded Norman R. Parmet as chairman, and Richard D. Blomberg replaced Mr. Johnstone as deputy chairman. John A. Gorham resigned as a Panel consultant, and Kenneth G. Englar and Captain Dennis E. Fitch were appointed as consultants. Mr. Melvin Stone retired as a Panel member and became a consultant to the ASAP. Dr. Seymour C. Himmel, formerly a consultant, became a member.

The balance of this report presents "Findings and Recommendations" (Section II), "Information in Support of Findings and Recommendations" (Section III) and Appendices (Section IV) describing Panel membership, the NASA response to the March 1995 ASAP report and a chronology of the Panel's activities during the reporting period.

II. FINDINGS AND RECOMMENDATIONS



II. FINDINGS AND RECOMMENDATIONS

A. SPACE SHUTTLE PROGRAM

OPERATIONS

Finding #1
Cutbacks in government and contractor personnel and other resources at the Kennedy Space Center (KSC) and the planned transition of tasks from government to contractor workers will create a new mode of Space Shuttle operations. Those involved in day-to-day Shuttle operations and management are in the best position to determine how to maintain the stated program priorities—fly safely, meet the manifest and reduce costs, in that order.

Recommendation #1
Additional reductions in staff and operations functions should be accomplished cautiously and with appropriate inputs from the KSC NASA/contractor team itself.

Finding #2
Obsolescence of Space Shuttle components is a serious operational problem with the potential to impact safety. Many original equipment manufacturers are discontinuing support of their components. NASA is, therefore, faced with increasing logistics and supply problems.

Recommendation #2
NASA should support augmenting the current comprehensive logistics and supply system so that it is capable of meeting Space Shuttle Program needs in spite of increasing obsolescence.

Finding #3
The Return to Launch Site (RTLS) abort maneuver is one of the highest risk off-nominal Space Shuttle flight procedures. A Space Shuttle Main Engine (SSME) shutdown leading to an intact abort is more likely than a catastrophic engine failure. Exposure of an ascending Space Shuttle to the risk of performing the demanding RTLS maneuver might be significantly minimized by operating the Block II SSME at higher thrust levels at appropriate times. Certification of alternative Space Shuttle landing approaches for use during contingency aborts and installation of Global Positioning System (GPS) could also contribute to the minimization of RTLS risk (see Finding #5).

Recommendation #3
NASA should pursue with vigor efforts to minimize Space Shuttle exposure to the RTLS maneuver through all available means.

Finding #4
The Range Safety System (RSS) destruct charges have been removed from the liquid hydrogen tank of the External Tank (ET). The risk studies which supported this removal also suggested that the RSS charges had to be retained on the Liquid Oxygen (LOX) tank of the ET. It is preferable to omit as much ordnance as possible from flight vehicles to reduce the possibility of inadvertent activation.

Recommendation #4
Studies supporting the need for the RSS destruct system on the LOX tank should be updated in light of the current state of knowledge, operating experience and the introduction of the new Super Lightweight Tank (SLWT) to determine if it is now acceptable to remove the ordnance.

ORBITER

Finding #5
The Orbiter and its landing sites continue to be configured with obsolescent terminal navigation systems. The existing Tactical Air Control and Navigation (TACAN) and Microwave Scanning Beam Landing System (MSBLS) systems are increasingly difficult to maintain, vulnerable and expensive. Continued reliance upon them limits landing options in the event of a contingency

abort. Replacement of TACAN and MSBLS with now available precise positioning GPS in a triple redundant configuration would ameliorate and most likely solve these problems.

Recommendation #5
Accelerate the installation of a triple redundant precise positioning service GPS in all Orbiters.

Finding #6
Orbiter Reaction Control System (RCS) *oxidizer* thruster valve leaks are occurring with increasing frequency. More recently, RCS *fuel* thruster valve leaks have also been observed. Because isolation of leaking thrusters can be implemented by manifold shut off and thruster redundancy is provided, leaking thrusters have not been considered a serious safety hazard. RCS leaks in the vicinity of rendezvous targets such as Mir and the International Space Station (ISS) could, indeed be a serious safety hazard.

Recommendation #6
Do what is necessary to eliminate the RCS thruster valve leaks now and in the future.

Finding #7
The use of Alumina Enhanced-Thermal Barrier (AETB) tiles with Toughened Uni-place Fibrous Insulation (TUFI) coating on the Orbiter has the potential to enhance safety and reduce life cycle cost.

Recommendation #7
NASA should make a thorough study of the potential use of the AETB/TUFI tiles in order to determine if it is cost effective to qualify the tiles for flight.

SPACE SHUTTLE MAIN ENGINE (SSME)

Finding #8
The SSME has performed well in flight during this year. While some launches were delayed because of problems or anomalies discovered during pre-launch inspections and checkout or development engine test firings at the Stennis Space Center (SSC), such issues were thoroughly and rapidly investigated and resolved.

Recommendation #8
Continue the practice of thorough and disciplined adherence to inspection and checkout of engines prior to commitment to flight as well as prompt and thorough resolution of any anomalies discovered.

Finding #9
The Block II engine, in near-final configuration, re-entered development testing in mid October 1995. Testing of what had been expected to be the final configuration was begun later that month. The High Pressure Fuel Turbopump (HPFTP) was a principal cause of the late restart of testing primarily because of slips in obtaining some redesigned turbopump components. The remaining time to achieve the scheduled first flight of the Block II configuration is very tight and allows for little, if any, problem correction during development and certification testing. The improved ruggedness and reliability of this version of the SSME is critical to the assembly and operation of the ISS.

Recommendation #9
Do not let schedule pressure curtail the planned development and certification program.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Finding #10
Post flight inspection of recovered RSRMs from STS-71 and STS-70 identified gas paths leading to primary O-ring heat erosion in joint #3 of the RSRM nozzles. Heat erosion in this joint could compromise Space Shuttle mission safety. NASA stopped all launches until the anomaly was resolved and corrective repairs made.

Recommendation #10
NASA should continue to investigate and resolve all potential Space Shuttle flight safety problems in this same forthright manner.

Finding #11
The schedule for firings of Flight Support Motors (FSMs) for evaluating changes made to the RSRM has been stretched out. Now, accelerating obsolescence and new environmental regulations have increased the need for the data supplied by FSM firings.

Recommendation #11
Do not further stretch out FSM firings.

EXTERNAL TANK (ET)

Finding #12
The development of the Super Lightweight Tank (SLWT) using Aluminum Lithium (Al-Li) material entails several unresolved technical issues. These include a low fracture toughness ratio and problems in large scale joint welding. There are also critical structural integrity tests which are behind schedule. Resolution of these issues could impact the delivery of the SLWT.

Recommendation #12
Satisfactory resolution of these issues must be achieved prior to SLWT flight.

B. INTERNATIONAL SPACE STATION

SHUTTLE/MIR

Finding #13
STS-74 delivered a Russian built docking module to Mir which will be used for multiple Shuttle/Mir dockings prior to ISS assembly. This docking module and one designed for use on the ISS use Russian-manufactured pyrotechnic bolts. These bolts cannot be certified to NASA standards because of the absence of adequate information from the manufacturer. They also do not meet the NASA design requirement that pyro bolts be hermetically sealed. The development of a replacement American pyro bolt has been put on hold because its design may violate the proprietary rights of the original Russian manufacturer.

Recommendation #13
Continue to pursue the options of having the Russian manufacturer modify the existing pyro bolt design to include a hermetic seal and the possibility of using the American designed pyro bolt as a substitute.

INTERNATIONAL SPACE STATION

Finding #14
Over the life of the ISS mission there is a risk of some meteoroid or orbital debris penetration. While there is an awareness of the need for mitigation of the potential for debris penetration of habitable and critical modules, planning and implementation of damage control and repair methods is lagging.

Recommendation #14
Continue to work hard to reduce the risk of penetration of inhabited modules by meteoroids or orbital debris. Implement damage detection, localization and isolation or repair measures to reduce the risk of life or mission threatening impacts.

Finding #15
The Caution and Warning (C&W) system design for the ISS has not kept pace with Station's level of development due to cost constraints among other reasons. As a result, the ability to develop a maximally effective safety system design which detects and localizes hazards and provides the information needed for damage control may be compromised.

Recommendation #15
The C&W system should not be unnecessarily constrained by other ISS design decisions or cost limitations. It is a vital part of the total safety environment of the ISS and deserves more detailed and timely design emphasis.

Finding #16
The decision by the ISS Program to use two Soyuz vehicles for crew rescue during the early years of deployment involves at least two significant limitations. The first is the exclusion of approximately 28% of the crew population due to anthropometric constraints. A second and more tractable issue is the acceptance by the Program of Russian language placards on displays and controls. Under pressure, rudimentary training in the Russian language has the potential to break down and increase the probability of errors.

Recommendation #16
There is little that can be done about the inherent limitations of the Soyuz design such as the crew size constraints until Soyuz is modified or replaced with a fully capable rescue vehicle design. The inclusion of some simple placards to provide English labeling would seem warranted given the emergency climate in which a rescue vehicle will be used.

Finding #17
The use of Soyuz as the Crew Rescue Vehicle (CRV) for the ISS provides only an interim capability. Maximally effective crew rescue capabilities can only be attained through

the development and deployment of a special purpose CRV.

Recommendation #17
A new, fully capable CRV should be developed and deployed as soon as possible.

Finding #18
There are important ISS data processing items for which there are no written requirements. For example, it appears that there is no formal requirement that any specific portion of the computational system, software included, be operational at any stage of ISS assembly.

Recommendation #18
NASA should review ISS top level requirements, and their flow down, and add specific requirements where necessary to assure the correct, staged, assembly of the station and its computer and software systems.

Finding #19
ISS computer system safety requirements, both hardware and software, have not been available in a timely manner to the product development teams. This is a matter of considerable concern. Also, the safety function of the Integrated Product Teams (IPTs) for computer system development appears less than totally effective.

Recommendation #19
NASA should review its computer system safety requirements and the integration of safety personnel into its IPTs to ensure that requirements are in place before they are needed, and that safety activities are given proper coverage.

Finding #20
While the ISS computer architecture has been simplified considerably, there are still areas in which problems exist. The planned lifetime of the Station will almost certainly require upgrades to various computer and avionics components, but there are no current plans for defining and managing upgrades.

Recommendation #20
NASA should have plans in place to test the robustness of the ISS computer architecture to ensure reserve memory and computing capacity throughout the Station's lifetime and to provide an upgrade path for critical computer system components.

Finding #21
Much of the testing for ISS software is based upon the use of simulators for various components. If the simulations are not correct, errors in the flight software could go undetected. The simulators are not subject to the same level of Verification and Validation (V&V) as the flight software. The V&V of the simulators is "by use" which means that the principal validation of the simulations occurs at the same time that the simulations are being used to perform V&V on the flight software.

Recommendation #21
NASA should employ methods for more thoroughly verifying and validating the simulation models used in V&V activities for ISS flight software.

Finding #22
It is not at all apparent that there are adequate and consistent controls on the software development tools that are in use for creating ISS software. For example, software being developed for Multiplexer/Demultiplexers (MDMs) will be written in Ada and compiled using a certified compiler while software for other device controllers may be written in a variety of languages and compiled with even an uncertified compiler. Also a commercial code generator is being used beyond its intended domain.

Recommendation #22
NASA should immediately review all of its software development processes and tools to ensure a consistent and adequate level of certification.

Finding #23
Initial ISS activities on Independent Verification and Validation (IV&V) of software appear to be following a logical and reasonable approach. The approach of bringing up issues at the lowest reasonable level and escalating up the chain of command as necessary is well advised and has been and should continue to be effective.

Recommendation #23
NASA should build upon the good start that has been made in the ISS IV&V effort.

Finding #24
The reduction in full around-the-clock support from the Mission Control Center, the likelihood of unanticipated safety situations to which the crew must respond and the extended mission durations suggest that the ISS strategy of deploying comprehensive on orbit training resources using both Computer Based Training (CBT) and Virtual Reality (VR) techniques is appropriate.

Recommendation #24
The ISS should continue its excellent strategy of using both CBT and VR training on orbit. In addition, an effective on-call system to ensure the rapid response of mission support personnel on the ground should be developed.

Finding #25
The currently proposed method for deorbiting/decommissioning the ISS at the end of its useful life entails a controlled, targeted reentry with surviving debris falling into a remote ocean area. The analysis and planning are based on having a fully assembled station and do not take into account deorbiting any of the possible configurations prior to completion.

Recommendation #25
NASA should develop plans for deorbit/decommission of intermediate ISS assembly configurations.

Finding #26
Current ISS plans include extensive Extravehicular Activity (EVA). As a result, NASA has planned an improvement program for the existing Extravehicular Mobility Unit (EMU) or space suit.

Recommendation #26
Continue to support the EMU improvement program to ensure that the EMU can meet the increased EVA requirements.

C. AERONAUTICS

Finding #27
The Congress has drafted legislation directing the privatization of the NASA microgravity research aircraft. No in-depth study has been completed on the safety ramifications of the transfer of the Johnson Space Center (JSC) KC-135 or Lewis Research Center (LeRC) DC-9 microgravity aircraft to commercial operation.

Recommendation #27
For reasons of safety, do not transfer any NASA microgravity research aircraft operations to a commercial provider until ongoing studies can assess the attendant safety issues. If economic or other reasons dictate that the aircraft must be transferred and time does not permit waiting for study results, then microgravity aircraft operations should be suspended until they can be certified safe under the aegis of the new operators.

Finding #28
Langley Research Center has commenced a joint Federal Aviation Administration (FAA)/ NASA program to amass data which can be used to formulate operational procedures for avoiding or minimizing the effects of flying into aircraft-generated wake vortices. This program has begun to shed light on an important area of flight dynamics suspected of having contributed to aircraft mishaps.

Recommendation #28
The wake vortex research program should be strongly supported and, whenever meaningful data are derived, these data should be exported to the National Transportation Safety Board (NTSB), the FAA and the entire spectrum of commercial, military and general aviation.

Finding #29
The Dryden Flight Research Center's *Basic Operations Manual* (BOM) describes a proactive attitude toward safety which is exemplary and worthy of emulation throughout NASA.

Recommendation #29
Other Centers and NASA contractors could profit from the use of the Dryden BOM as a model.

D. OTHER

Finding #30
NASA researchers have examined the impact of fatigue and circadian disruption on pilots and shift workers and developed a *Fatigue Countermeasures Program*. Material developed by the *Fatigue Countermeasures Program* is now in widespread use at airlines and elsewhere. Tens of thousands have received training and guidance on effective ways to manage fatigue through symptom identification and scheduling/behavioral, physiological, pharmacological, and technological countermeasures.

Recommendation #30
Methods for fatigue identification and material on effective fatigue countermeasures should be incorporated in training including that for astronauts, flight crews, ground crews and mission controllers. These groups are often forced to vary their work hours and could therefore benefit from the information now widely being used throughout the transportation industry.

Finding #31
The *Senior Managers' Safety Course* conceived and conducted by JSC is an outstanding overview of philosophies, techniques and attitudes essential to a successful safety program.

Recommendation #31
A safety course for senior managers similar to the one conducted at JSC should be established at other NASA centers and Headquarters. Consideration should also be given to exporting the course to major NASA contractors and including its elements in managerial training programs.

Finding #32
NASA's ongoing reorganization and the intention to pass responsibility for Space Shuttle operations to a single Space Flight Operations Contractor (SFOC) have potential safety implications. To this point, other than an effect on morale at the KSC due to uncertainty, no significant problems have surfaced.

Recommendation #32
NASA leadership and top management should continue active and detailed involvement in the safety aspects of planning for and oversight of the NASA reorganization in general and Space Shuttle operations in particular.

Finding #33
The plan for Space Shuttle restructuring and downsizing provides that NASA personnel will be involved in the resolution of any off-nominal events which are beyond the operating experience base or "out-of-family." This places extreme importance on the development and implementation of the definition of an out-of-family situation.

Recommendation #33
NASA personnel with direct Space Shuttle operations experience should be involved not only in the derivation of the definition of out-of-family but also in the day-to-day decisions on what constitutes an out-of-family event.

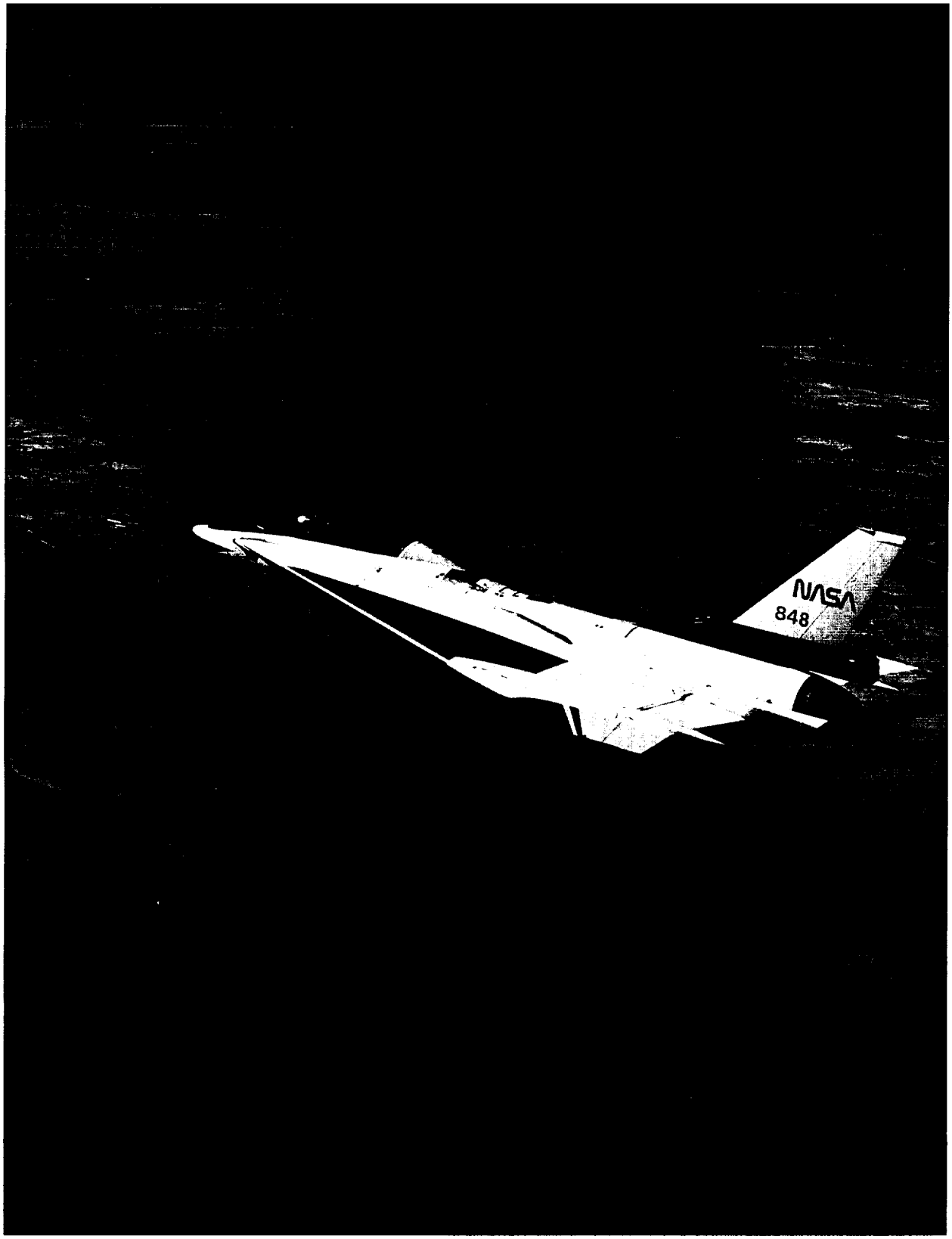
Finding #34
New propulsion control modes utilizing neural nets are under development. The use of neural nets raises questions of how such control software are to be verified and validated for flight operations. There may be a technology/certification mismatch at present.

Recommendation #34
The Ames Research Center in its capacity as designated center of excellence for information systems technology should undertake the research and technology necessary to provide NASA with appropriate V&V techniques for neural net control software.

Finding #35
While hardware typically gets adequate coverage from the Safety and Mission Assurance organizations at the NASA Centers, there is evidence that software does not.

Recommendation #35
The Headquarters Office of Safety and Mission Assurance should examine the depth of the software assurance process at each of the Centers and promulgate NASA-wide standards for adequate coverage.

III. INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS



III. INFORMATION IN SUPPORT OF FINDINGS AND RECOMMENDATIONS

A. SPACE SHUTTLE PROGRAM

OPERATIONS

Ref: Finding #1

The work force at the Kennedy Space Center (KSC) performs by far the largest "touch labor" on the Space Shuttle. As such, their performance is a major determinant of the safety of operation of the vehicle and its systems. In addition, many of the pre-launch and launch preparations involve hazardous operations such as the handling of hypergols. Distractions which cause less than a total focus on the work at hand can result in significant industrial safety problems.

The announcements of plans for additional cutbacks and a significant restructuring of Space Shuttle launch responsibilities under a single Space Flight Operations Contractor (SFOC) have the potential to affect worker morale at KSC. The resulting state of flux and uncertainty in the Space Shuttle Program creates a climate in which safety ***might*** be compromised. Cutbacks which result in lost jobs and uncertain futures, both for the Program and individual workers have the potential to undermine morale. Proposed fundamental changes in the structure of the system can lead to the inadvertent omission of vital process steps. It is impossible to define clearly at what point the Program will cross over from safe to unsafe conditions, but this crossover would surely occur if reductions are allowed to proceed uncontrolled.

In spite of the negative potentials, assessments by a special team from the Panel suggest that the commitment of Space Shuttle personnel to safety above all else remains intact. This holds for management and workers and for both contractor and NASA personnel. To be sure, morale is down and distractions are up, but as long as the existence of the Space Shuttle Program is assured, professionalism should prevail with resulting safe operations. It seems abundantly clear that schedules may be sacrificed, but safety will not knowingly be compromised.

With respect to the proposed transition plans, there is no inherent reason why any reasonable Space Shuttle structure cannot be consistent with safe operations. Restructuring the Space Shuttle Program can be accomplished while maintaining safe operations, provided it is approached cautiously and based on the extensive lessons learned from past safe Space Shuttle operations. The Space Shuttle systems and organization must therefore be changed with care and with a complete awareness that what might work for a totally new organization may not be fully applicable to the overhaul of one which has been operating successfully for so long.

There are several principles which the Panel believes must be followed in any Space Shuttle Program transition process:

- First, the ***team*** approach to Space Shuttle decision-making involving both NASA and contractor experts should be maintained. It has functioned effectively and provides the checks and balances which are essential to the operation of such a complex enterprise.

- Second, additional reductions in staff and operating functions must be made judiciously ***by the team itself*** based on definitive statements of operating objectives and funding guidance from Congress and NASA management. Those involved in day-to-day Space Shuttle operations and management are in the best position to determine how to take cuts without unduly impacting safety.

- Third, organizational change must be gradual and also managed by the ***team.*** Adequate time must be allocated for analyzing the effects of changes as they are made and permitting the system to reach new equilibrium points. This will ensure that vital safety systems are retained or replaced by suitable substitutes.

In short, the Space Shuttle Program appears to be properly managing risk. Hardware upgrades already in work, such as the Block II main engines, will provide even greater safety enhancements. The Program has successfully shed significant costs and can likely reduce expenditures even more without materially increasing risk as long as change is properly managed, given ample time and guided by those with first hand knowledge of Program operations.

Ref: Finding #2
The realities of supporting the Space Shuttle today are dominated by issues related to obsolescence. These issues can be divided into three broad categories:

- Obsolescence due to life limits or wear out of components and, in some cases, functional systems. This includes industry's abandonment of systems which were state-of-the-art in 1970 when they were adopted for the Space Shuttle.

- Obsolescence due to stringent new environmental requirements, especially with regard to repair and overhaul processes. The disposal and control of hazardous waste also impose a new dimension upon the support tasks.

- Obsolescence due to the inability to support component overhaul and repair because vendors have gone out of business or cannot support the Space Shuttle, for example, due to loss of skills and specific experience or unavailability of special parts.

Examples of current difficulties include a number of important avionics components (e.g., master event controller, signal processing assembly, several tape recorders) and airframe components, (e.g., CO_2 sensors, H_2/H_20 separators, water spray boilers, ammonia boilers). Major items such as the Auxiliary Power Units (APUs) are struggling from crisis to crisis in many cases due to subcomponent problems, and the Orbital Maneuvering System (OMS) pod problems are continuing.

Tracking and control systems for the multiplicity of logistics problems appear to be providing adequate information, but coping with the increasing obsolescence trends will inevitably lead to a higher rate of cannibalization or to "workarounds" which might impair safety. Better visibility into the entire subject of obsolescence should be developed if NASA is to avoid crises in the future.

Ref: Finding #3
Return to Launch Site (RTLS) requires an unusual and demanding flight profile fraught with the potential for error in a high stress abort situation. Should there be a shutdown of a main engine during the early part of the ascent, the RTLS procedure requires that the Space Shuttle continues powered flight after separation of the solid rocket boosters to expend propellants and then jettison the External Tank (ET). After solid rocket booster jettison, a powered pitch around must be performed so that the orbiter is literally flying backwards so that the thrust of the remaining Space Shuttle Main Engines (SSMEs) can supply a braking force. This is followed by a powered pitch down, a pullout and entry into the landing maneuver. All of this adds up to extremely complex flight dynamics including the need to fly through the SSME plume and its associated turbulence, heat and other off nominal flight dynamics. Remedies might include the following:

- Demonstration of operation of the SSME Block II at settings greater than 109% for use during an intact or contingency abort.

- Investigation of the thermal and structural loads to which the Space Shuttle would be subjected at higher power settings.

- Installation of a certified three string Global Positioning System (GPS) capability.

- Investigation of changes in planned landing trajectories including so called stretched entries.

While the above actions all contribute to the safety of the Space Shuttle during ascent by minimizing exposure to the necessity for RTLS, each one by itself also contributes to the enhancement of safety in other Space Shuttle flight regimes. NASA's response to the Panel's recommendation on the same subject last year stated that an SSME certification at higher power settings was underway. This year's investigation did not reveal a coordinated program to minimize RTLS exposure.

Ref: Finding #4
The original design of the Space Shuttle included Range Safety System (RSS) destruct charges on both the Liquid Oxygen (LOX) and Liquid Hydrogen (LH_2) tanks of the ET. These were to be used in the event of an accident to ensure the complete destruction of the tank elements before impact and therefore protect the safety of people and property on the ground.

There is some added risk to the crew associated with flying with destruct ordnance on the vehicle. The crew would therefore prefer to reduce their exposure to risk by eliminating the RSS charges. Some time ago, NASA commissioned studies by the Naval Surface Warfare Center which provided data which led to the conclusion that the risk to people on the ground (or ships at sea) from the LOX tank was unacceptably high in the event of certain aborts unless the LOX tank was destroyed by ordnance. These same studies were used to support the removal of the destruct charges from the LH_2 tank as analysis indicated it would break up prior to impact even without a destruct charge.

Based on the Navy's studies, the Air Force Eastern Test Range concluded that the charge on the LOX tank could be ejected or safed after first stage for low inclination launches. It was, however, needed for high inclination launches and during first stage. The Space Shuttle Program chose to retain the charge rather than increase system complexity with a charge that could be disarmed or ejected in flight.

The Space Shuttle has now amassed significant additional operating experience. The assumptions used in the original Naval Surface Warfare Center studies may, therefore, no longer be totally operative. The situation at present may favor removing the charges from the LOX tank to reduce risk to the crew. At very least, given the concern of the Astronaut Office and some senior NASA engineers, it would seem wise to revisit the underlying studies and their assumptions to determine if they are still valid in the current operating environment. Intermediate possibilities such as a software patch or other Safe and Arm mechanism to disable the RSS system and protect it from stray radio signals after first stage should also be considered.

ORBITER

Ref: Finding #5
While a decision has in fact been made to equip Orbiters with GPS, and a stretched out program of single string installation and testing is in place, the current plan will not complete a three string system in even one vehicle until the year 2000. Reasons for delay include money availability and a perceived need to await an Orbiter Maintenance Down Period (OMDP) for installation of certain wiring and antennas.

With a fully redundant precise positioning service GPS in operation (a capability now guaranteed by way of a NASA/DOD memorandum of understanding), landing the Orbiter only at sites where TACAN and MSBLS are maintained would no longer be a constraint. With GPS any airfield with adequate runway length anywhere within the Space Shuttle footprint would be a potential landing site.

An additional and important reason to accelerate GPS installation centers on the fact that MSBLS is suffering from an inability to be repaired at the Shop Replaceable Unit (SRU) level. While SRUs can still be purchased, this is becoming increasingly difficult. Also, it was recently learned by the Panel that Orbiter TACANs are made by two different companies thus even further complicating logistics and, potentially, system reliability.

Ref: Finding #6
Orbiter Reaction Control System (RCS) *oxidizer* thruster valve leaks are occurring with increasing frequency. Most recently, RCS *fuel* thruster valve leaks have also been observed. Because isolation of leaking thrusters can be implemented by manifold shut off and thruster redundancy is provided, leaking thrusters have not been considered a serious safety problem. RCS leaks in the vicinity of rendezvous targets such as Mir and the International Space Station (ISS) could, indeed be a serious safety hazard.

The principal cause of leaking thrusters is iron nitrates that accumulate on the valve seats and/or poppets of the main and pilot stages of the oxidizer valve. The current pilot-operated valve is particularly susceptible to this nitrate contamination. In spite of actions to upgrade maintenance and handling procedures for the RCS thrusters, leakage persists. Given the increasing importance that the RCS thrusters will play in future missions, NASA should do whatever is necessary to eliminate the RCS thruster valve leaks now and in the future.

Ref: Finding #7
The Alumina Enhanced-Thermal Barrier (AETB) tiles with Toughened Uni-place Fibrous Insulation (TUFI) coating have higher temperature capability, improved durability and dimensional stability and can be manufactured in various densities from 8 to 22 lbs/ft^3.

The TUFI coating which is impregnated into the tile surfaces provides improved impact resistance and greater durability. It also reduces handling damage, maintenance, cost and repair time. The evaluation of TUFI on existing tiles began in 1994 with flight demonstrations on OV-102 and OV-103. There are a large number of current tiles on the Orbiter that if replaced with AETB/TUFI at 8 lbs/ft^3 might save inert weight in the Orbiter.

While AETB/TUFI tiles have the potential to increase capability substantially and save weight at the same time, they are not qualified for use on the Orbiter. NASA should plan to qualify the AETB/TUFI tiles for flight making maximum use of the data base from the qualification of the current tiles.

SPACE SHUTTLE MAIN ENGINE (SSME)

Ref: Finding #8
The Space Shuttle Main Engine (SSME) has performed well in flight this year. There have been, however, a number of instances where anomalies found during pre-flight checkout or in development tests at the Stennis Space Center (SSC) have caused launch delays while the causes were determined and corrective action or additional inspections were implemented.

For example, on STS-73, which had been scheduled to fly three Block I engines, one of the engines had to be removed because it could not be verified while the engine was installed on the Orbiter that an internal seal on its High Pressure Oxidizer Turbopump (HPOTP) had been installed properly on that particular engine. The potential for such a mis-installation was discovered in the factory and an additional inspection had been added to the manufacturing process to assure that the seal was installed correctly. Unfortunately, the pump on the engine in question had been installed prior to the implementation of the new inspection which led to the removal and replacement of the engine, delaying the launch.

Another incident occurred on an engine in a test stand at SSC in the process of starting a development test firing. A leak occurred in the high-pressure discharge duct from a HPOTP, and the test firing was aborted. A failure investigation found that there was a rather large crack in the duct at the site of a weld. It was revealed that when the weld bead had been ground down ("flushed") as part of the manufacturing process, some of the parent material had been removed making the wall section too thin. After considerable operating time, high-cycle fatigue set in and the crack and leak occurred. All engines, including those installed on an Orbiter ready to launch, were then subjected to ultrasonic inspection to verify adequate wall thickness. This, of course, occasioned a launch delay.

The importance of the above is to note that the program has continued its devotion to safety of flight by insisting that all such occurrences are investigated thoroughly and any corrective action or special inspections are implemented before commitment to flight. Such a disciplined approach to problem resolution must continue.

Ref: Finding #9

The Block II engine comprising the Block I configuration plus the Large Throat Main Combustion Chamber (LTMCC) and the Advanced Turbopump Program (ATP) High Pressure Fuel Turbopump (HPFTP) re-entered development testing in near-final configuration in mid-October, 1995 after authority to re-start the activity was given in the spring. The delay in starting the development and certification test program was caused by slips in the schedules for producing modified HPFTP components. Included among the redesigned components were: the turbine vane assembly change from 54 to 75 vanes (to provide correct turbine flow area as well as to de-tune the flow perturbations from a dynamic mode of the turbine blades) and changes to the second stage turbine vanes (to eliminate cracking at the junction of the leading edge of the vanes with the back-up structure).

The first test of this configuration yielded excellent results with turbine temperatures and other performance parameters of the HPFTP equal to or better than predicted. The Specific Impulse (I_{sp}) achieved in this test was better than the specification indicating that the slight loss of I_{sp} experienced with the Block I engine had been overcome. There was only slight blanching of the LTMCC which can be corrected easily.

The penultimate configuration Block II engine started testing subsequently. This configuration contains an ATP HPFTP with all but one of the planned design changes incorporated and the final version of the LTMCC which includes the cast manifolds. The one HPFTP change not included is a damper for the lift-off seal which may not be needed if testing so indicates. Early test results of this configuration revealed a number of problems associated with mechanical details of the turbopump. Fixes for these problems have been devised but implementation will impact the schedule. It was anticipated that the test program could be resumed by early 1996. On the positive side, the specific impulse deficit experienced on the Block I configuration has been overcome and the LTMCC is achieving better than specified performance.

At the time of this writing, the Block II engine program was three to four months behind its original schedule. This leaves very little room for problem resolution during this activity if the program is to meet the planned Block II first flight in September 1997. The more robust and reliable Block II engine is vital for the Space Shuttle support of the assembly and operation of the ISS and every effort must be made to keep the development and certification of this engine configuration on schedule.

REUSABLE SOLID ROCKET MOTOR (RSRM)

Ref: Finding #10

Several past instances of gas paths leading to *soot* on the primary O-ring in RSRM nozzle

joint #3 were observed during post flight inspections. These "out of family" instances showed no evidence of *heat* eroding the nozzle primary seal, nor was it considered a likely occurrence by NASA or the RSRM contractor, Thiokol. The "blow-by" was thought to be permitted by compressed air pockets remaining in the Room Temperature Vulcanizate (RTV) thermal barrier installed during assembly of nozzle joints #3 and #4. Such voids could provide an easy pathway for exhaust gases to reach the joint O-ring.

Tiny burn marks were found on the joint #3 O-rings in three of the four STS-71 and STS-70 RSRM nozzles prompting a renewed investigation of the anomalies. Mission managers put the next Space Shuttle launch, STS-69, on hold while the situation was reviewed. A special industry/ NASA committee was convened. The in-depth investigations by this committee verified that the hot gas paths which caused heat erosion of the primary O-rings resulted from the RTV backfill process employed during nozzle assembly. A worst case thermal environment analysis of a single hot gas path to the primary O-ring demonstrated that there would be insufficient energy to burn through the primary O-ring during flight. Nevertheless, the committee recommended inspection and repair of the joints prior to flight even on already assembled nozzles.

A repair procedure to remove and replace the original RTV in nozzle joints #3 and #4 was developed to eliminate all "tail" voids above the joint inflection point thus reducing the potential for providing a gas path to the primary O-ring during RSRM operation. The repair procedure was validated on two flight configured nozzles at Thiokol's Utah plant and then used to repair the STS-69 boosters on the launch pad and clear them for flight. Post flight analysis of STS-69 SRM's found no gas paths to the primary O-rings in any of the four repaired joints.

Subsequently, the remaining RSRM nozzles awaiting flight were repaired and the assembly process in the plant was modified to avoid the problem. NASA should continue to investigate and resolve all potential Space Shuttle flight safety problems in this same forthright manner.

Ref: Finding #11
The firing of Flight Support Motors (FSMs) has been stretched out from a one to a two year interval. These firings are used to qualify design changes and new materials which must be introduced due to environmental regulations and obsolescence. Accelerating obsolescence and new environmental regulations have increased the need for the data supplied by FSM firings. Because of their importance in ensuring the safety of the RSRM, the FSM firings should not be stretched out any further.

EXTERNAL TANK (ET)

Ref: Finding #12
There are a number of technical issues that could affect the margins of safety of the Super Lightweight Tank (SLWT). Normally the design of a structure is based on well characterized materials with statistically derived design allowables from sufficient tests. The Aluminum-Lithium (Al-Li) material for the SLWT is not well characterized. Its properties therefore are being validated by lot acceptance and structural tests. Unresolved technical issues include a low fracture toughness ratio and problems in large scale joint welding.

The yield to ultimate stress of 2195 Al-Li material is less than the original 2219 Al material which results in reduced fracture toughness characteristics. The fracture toughness ratio is of concern because the Al-Li material being received exhibits properties

inferior to the design values used. It may be necessary to perform special fracture toughness material tests to simulate service. There are still a number of material tests that must be conducted to verify the suitability of the Al-Li material. These include fracture toughness ratio tests.

Remaining structural integrity tests which must be performed include proof tests and a test of the aft dome to ultimate to verify its buckling strength. The Aluminum Lithium Test Article (ALTA) will be used to demonstrate the ultimate strength capability of the structure. At present this test is behind schedule and personnel are working overtime to recover. Finally, there are protoflight tests that will be performed on the LO_2 and LH_2 tanks which should ensure their suitability for flight.

B. INTERNATIONAL SPACE STATION

SHUTTLE/MIR

Ref: Finding #13
STS-74 delivered a Russian built docking module to Mir which will be used for multiple Shuttle/Mir dockings prior to ISS assembly. This docking module and one designed for use on the ISS use Russian-manufactured pyrotechnic bolts. The Russian pyro bolts cannot be certified for multiple flights because of outgassing. Current sealing of the pyro bolts is inadequate. In a vacuum, they outgas to the extent that the explosive charge may be insufficient to sever the bolt. Outgassing may also cause the explosive to become brittle, crack, and inadvertently detonate due to electrostatic discharge or friction. Conversely, while on the ground the explosive charge may soak up enough water to cause it to dud (no fire).

The most desirable way forward is to use an American pyro bolt with known characteristics which can be certified. If this cannot be achieved because of legal constraints, adequate hermetic sealing of the Russian pyro bolt is required.

INTERNATIONAL SPACE STATION

Ref: Finding #14
The overall design philosophy for the ISS to mitigate the effects of meteoroid/orbital debris (M/OD) impacts has been formulated and is being implemented throughout the program. In essence, habitable and critical pressurized modules will be protected by shielding against penetrating impacts of particles of the order of 1 cm in diameter and smaller. These represent the vast majority of M/OD objects found at ISS operating altitudes. Objects of the order of 10 cm and larger are tracked and cataloged by the US Space Surveillance Network. The plan for this size range of object is to obtain warnings from the Network of close approaches of objects and, using an altitude reboost engine burn, to maneuver the ISS out of a possible collision path. The remaining objects, from 1 to 10 cm in size, are a very small population and constitute the residual threat of penetration with no protection other than the statistically small chance of encounter.

Since the probability of penetration of some habitable or critical module remains finite (about 10–20% over a 10 year mission life), further measures must be taken to limit and control damage after it occurs. Identification of such measures is presently underway, but implementation is still in the early planning stage. An integral part of such a scheme should be identifying and providing instrumentation for detecting and locating penetrations and development of the means for isolating and repairing damage. As of December 1995, there are no plans for such instrumentation, nor is it clear that there is a specific requirement for it (see Finding #15).

The concern is that by the time damage control procedures are worked out and supporting instrumentation is identified, there will be insufficient time to incorporate them into the design, thus leading to inadequate risk mitigation.

Ref: Finding #15
The Caution and Warning (C&W) system design for the ISS will play an important role in preserving the safety of the crew. At the time of this writing, it appeared as though the definition of the C&W was not consistent with the level of maturity of some of the other ISS systems. C&W design should not be an afterthought. In order to include the maximum extent of protection for the crew, it is important to make the C&W design an integral part of the ISS development.

To meet its objectives, a C&W system must adequately address the functions of hazard detection, hazard localization and crew notification of both the nature and severity of the event. If these objectives are achieved, a crew

will have the maximum chance of surviving a hazardous event, and their ability to control damage will also be maximized. The ISS requirements specify that its C&W system must address threats from fire, toxic spills and depressurization. These are the main hazards facing the crew.

The present C&W design does not appear to provide sufficient localization information and incorporates suboptimal annunciation methods. It appears as though significant needed capability has been omitted due to cost constraints and because of steadfast adherence to previously accepted rules which can no longer be supported in the present budget climate. The present design does not even include scarring for the later addition of increased capabilities.

The Personal Computer System (PCS) or "laptop" which is part of the ISS design is an example of a system which has some enhanced capability for annunciation to the crew. The problem is that the PCS as currently specified does not meet the rigid reliability specifications for dedicated computer gear. Single Event Upsets (SEUs) are a particular concern. These are temporary computer lock-ups caused by radiation particle hits. The computer must be re-booted before it can be used again. The alternative to using the PCS for localization information is to rely on a fixed C&W panel on the wall of each module which provides only minimal information to the crew and requires them to translate some distance to obtain it.

The current limitation of the PCS to only Criticality 3 (crit 3) functions appears worthy of reconsideration. It is apparently based on logic such as: 1) off the shelf the PCS is subject to some SEUs and somewhat lower reliability than a true "space hardened" piece of hardware; 2) space hardened hardware is expensive; 3) the money is not available; 4) non-space hardened hardware can be used for non-critical functions; 5) therefore, the PCS will be relegated to crit 3. The potential fallacy in this argument is that it ignores crit 2 and even crit 1 functions which are not being handled anywhere else in the system. For example, it might be preferable to use the PCS for C&W localization functions, even with a relatively high (but absolutely small) chance of locking up due to SEUs, than not to have the localization at all.

It would seem wise for the ISS Program to explore again the tradeoff between using a device such as the PCS which has a higher risk of unreliability than has been traditionally accepted and omitting the needed information altogether. Given the relatively low chance of a PCS failure and the almost certain ability to detect the failure if it does occur, it might be advisable to waive the stringent reliability requirements and use the PCS to its full potential. If it were to fail, the system would merely degrade to the currently planned and accepted performance level.

The present ISS design also does not provide for the localization of depressurization events. In the absence of this information, the crew will certainly be delayed in determining appropriate countermeasures for their own safety and to preserve the ISS in case of a depressurization. Space Station Freedom had a plan for localizing a depressurization event using airflow directions and velocities. This may be difficult and/or expensive to implement under the ISS architecture, but it is certainly technically feasible. Some level of localization of pressurization information should be considered as part of the ISS C&W design.

Ref: Findings #16 and #17

Soyuz has been specified as the initial Crew Rescue Vehicle (CRV) for the ISS. It is obvious that Soyuz is the only CRV which can reasonably be available for the first years of the ISS mission. The use of Soyuz, however, involves several limitations which should not be minimized. The first is the exclusion of

28% of the US astronaut population because of anthropometric constraints. There is little that can be done about this without modifying or replacing Soyuz, but NASA should at least acknowledge this as a consequence of its use. Crew members exceeding the anthropometric limits imposed by Soyuz will not be able to remain on the ISS until Soyuz is replaced by a new CRV.

A second and more tractable issue with the use of Soyuz is the acceptance by the program of Russian Language labeling on displays and controls. It is not clear why some simple placards cannot be added to provide English labeling. This would certainly seem warranted given the emergency climate in which a CRV will be used. Under pressure, rudimentary training in the Russian language has the potential to break down and increase the probability of errors.

The Panel position presented last year must also be reiterated: that use of the Soyuz as an interim measure is only justifiable as an expedient from the standpoint of safety. A new and more capable crew rescue vehicle is definitely needed to minimize risk over the operational life of the ISS.

Ref: Finding #18

The principal mechanism that NASA and its contractors use to ensure the completeness of their designs is the traceability of requirements. All of the specific work items are expected to trace back through a requirements flow down. If a task cannot be traced through a requirements flow, then there is no requirement that the task be accomplished. A concern is that there are important items for which there are no specified requirements. Curiously, there is no formal requirement that the space station be assembled or be operational after each stage. Consequently, there are no requirements concerning what portions of the software must be operational at the completion of each stage. It appears that there is no formal requirement that any specific portion of the computational system, software included, be operational at *any* stage.

The absence of detailed requirements makes it difficult to organize software development in such a way as to guarantee that the station computer systems will be operable after each assembly stage. For example, the top level flight-by-flight computer requirements for ISS assembly occur at the software requirements specification level. The Guidance, Navigation and Control (GNC) requirement for ISS is above that level. Thus, there is no formal requirement in the requirements flow down that GNC functions be operable before Assembly Complete. This is being handled in an ad hoc manner at present. It appears to be the case that the analysis and integration teams (AIT's) are supposed to be looking for things like this. However, this mechanism seems rather loose, leading to concern that something important may be overlooked. NASA should therefore review ISS top level requirements, and their flow down, and add specific requirements where necessary to assure the correct, staged, assembly of the station and its computer and software systems.

Ref: Finding #19

There are several situations which indicate that the safety process is not integrated into ISS computer system development in an effective and meaningful way. It was reported to the Panel that computer safety requirements did not flow down to the Integrated Product Teams (IPTs) until September 1995. The lack of safety requirements has been a matter of considerable concern to the ISS computer development IPTs. Nevertheless, while awaiting formal requirements the teams are working to what they expected them to be in the hope that major changes would not be necessary when the safety requirements were received.

Apparently, there is also not an effective integration of the safety function within the product

teams. For example, at the time of this writing no integrated schedule for software development across the various assembly stages existed. This may be an outgrowth of the general issue of lack of requirements, not just formal safety requirements, but functional requirements that have safety implications. It would seem that these situations are a result of tight schedules, time pressures and limited budgets. While the specific issue of safety requirements is presently scheduled to be resolved by the time of publication of this report, it is the broader perspective of the accumulation of many different unresolved issues that is of greatest concern. It appears that computer system safety may not be receiving the level of attention it deserves. Overall, it is not clear that the processes needed for the development of safe and functional computer systems are in place.

Ref: Finding #20
The ISS computer architecture has been simplified considerably from the early days of Space Station Freedom, mostly for the better. However, there are still areas for concern. Perhaps these concerns are transient and may be removed as development progresses. Nevertheless, their existence at this late stage of development is worrisome.

The backbone of the ISS computer system architecture is a standard 1553 data bus. This technology has been in use in the military for more than a decade and is considered proven. However, NASA is building the largest 1553 network ever constructed, and is finding serious problems, even when everything is "within specs." For example, the simple operation of inserting a new node on the network or moving the physical location of a node by a foot or two may be sufficient to make the network fail. It is presumed that the specified network will be made to function correctly. But, how robust will it be? How will it behave on orbit under varying conditions? How will it function after it must be repaired on orbit?

There are also significant computer capacity issues at present. In particular, some memories are more than fully subscribed. Scrubs are taking place, and must be monitored carefully to ensure that needed capability is not removed.

There are no plans for upgrading the processors. The specified processors employing "386" technology are already near the end of their lifetime and will be past the end by the time the ISS is complete. Plans have been made for upgrading memory and other components but not the Central Processing Unit (CPU) itself. Moreover, the use of a 16 bit bus is a throwback to older technology.

Ref: Finding #21
The testing of ISS integrated software systems is highly dependent upon the use of simulation. This is essential since in some cases, it is not possible to integrate everything on the ground. The validation of the simulation models is critical to the success of the testing process. The plan for ISS is to validate the simulation models "by use." That is, each model is validated by how well it appears to perform when it is used in the validation of ISS software during simulations. A safety concern with this approach is how it can be determined that the fidelity of the model is adequate. Given the safety criticality of much of the ISS software, NASA should employ methods for more thoroughly verifying and validating the simulation models used in Verification and Validation (V & V) activities for ISS flight software.

Ref: Finding #22
It is not at all apparent that there are adequate controls on the software development systems that are in use for creating ISS software. The software developed for the Multiplexer/ Demultiplexers (MDMs) will be written in Ada, and compiled using the Alysis compiler, for which a certification process has been used. This seems reasonable. However, there

is a great deal of software that will be in device controllers other than the MDMs. This latter software may be written in the C language and compiled with virtually any C compiler. There are no requirements for certification of the C compilers used, nor even a requirement that the same compiler be used throughout.

One of the emerging techniques for developing large software systems is the use of domain specific (e.g., control systems) code generators. Matrix X is such a system that is being widely used for ISS code development. For its intended domain, this is fine. However, Matrix X is being used extensively for applications beyond those for which it was designed and for which it may produce inefficient, and certainly less well tested, code.

There is also considerable code from Space Station Freedom that will be used. In the case of this code, the testing and validation is being "grandfathered" based upon previous testing. This may not result in any problems since it appears that the testing and validation for Freedom were more rigorous than for ISS. However, it was reported that the available test records are sometimes incomplete.

The ISS software is not all being developed by NASA and its contractors. The Russians are developing the software for the service module and will use a different processor. The possibility of integrating one more type of hardware and operating system presents a potentially daunting technical challenge.

In view of the above, NASA should immediately review all of its ISS software development processes and tools to ensure a consistent and adequate level of certification and adequate functional integration.

Ref: Finding #23
Initial ISS activities on Independent Verification and Validation (IV&V) of software appear to be following a logical and reasonable approach. The IV&V contractor seems to be well on board and establishing relationships with the program so that they can have access as the work proceeds. They have decided not to attempt to bite off more than they can chew and have developed what appears to be an acceptable approach to the job. Having half their work force at the Johnson Space Center (JSC) is good and is vital to their effectiveness. Their approach of bringing up issues at the lowest reasonable level and escalating up the chain of command as necessary is well advised and should be effective.

The initial IV&V work focused on a number of programmatic issues and provided good insights into some real program problems. Once requirements are finalized, it is hoped that IV&V efforts will turn to analyses of the software itself.

Ref: Finding #24
The plans for the ISS involve extended mission durations. It will not be efficient or cost effective to provide weekly 21 shift "full" coverage at the Mission Control Center (MCC). NASA should evaluate staffing requirements shift-by-shift and arrange work schedules accordingly. The development of a plan for reduced staffing might profitably benefit from examining the methods used by the airlines in analogous situations.

In the event of a problem on the station, the crew will have to respond based on its training and the support it receives from technical experts on the ground. It is likely that some of the responses to off-normals will have to be made during a reduced staffing shift in the MCC. It is possible that the crew may have to respond to something they were not trained for or for which refresher training is needed. Computer Based Training (CBT) and Virtual Reality (VR) techniques will permit the crew to prepare adequately for the necessary

response in a timely and efficient manner regardless of the level of immediate support available from the ground. Advances in both CBT and VR technologies have rendered these approaches fully "operational" and well within the resource constraints of the ISS. The continued use and expansion of both CBT and VR training techniques would therefore appear appropriate.

Ref: Finding #25

The currently proposed method for deorbiting/ decommissioning the ISS at the end of its useful life entails a controlled, targeted reentry with surviving debris falling into a remote ocean area. This requires that some sort of propulsive module will be available very early in the assembly sequence in order to have the capability for controlled reentry. The technical feasibility of this approach is covered in *Draft Tier 2 Environmental Impact Statement for International Space Station* dated October 1995 and is based on having a fully assembled ISS in orbit.

The assessment does not take into account any potential cases where the station is less than 100% complete. Between the first element launch in December 1997 and the fully assembled ISS in 2002, there will be several significantly different configurations. A controlled reentry of some of these configurations might be essentially the same as that of the completed ISS; however, there are likely to be other situations where reentry characteristics will be significantly different from those of the fully assembled station.

Also, it is possible that the reentry of the ISS, whether complete or incomplete, could be inadvertent. The behavior of any ISS configuration during an inadvertent reentry would be expected to be similar to that of its counterpart during a controlled deorbit sequence except for the landing area. The difference lies only in the indeterminate location of the impact area/footprint under the orbit flight path as opposed to the predetermined remote ocean location that would be preferred for decommissioning. An inadvertent reentry could occur if: 1) there was an inability to supply the propellant required to maintain a safe orbit; 2) there was a disabling collision with orbital debris, meteoroids or other objects; or 3) there were multiple major on-board failures. Therefore, NASA should develop plans for deorbit/decommission of intermediate ISS assembly configurations with or without control capability.

Ref: Finding #26

As plans for the ISS mature, it is clear that extensive Extravehicular Activity (EVA) will be required to assemble and maintain the station. In order to support these EVAs, an upgrade program for the Extravehicular Mobility Unit (EMU) or space suit is needed. NASA has identified the key components of this program including extending the number of uses between overhauls, permitting some on-orbit sizing and improving the gloves and the Portable Life Support System. Given the importance of the EMU for safe EVAs, NASA should continue to support the EMU improvement program to ensure that it can meet increased EVA requirements.

C. AERONAUTICS

Ref: Finding #27
The Congress has drafted legislative language directing that NASA's microgravity aircraft operations be privatized. There is great concern among the Panel, the NASA Intercenter Air Operations Panel and the NASA microgravity aircraft operators over safety should a new, inexperienced operator enter upon the scene. Microgravity flying, especially with large aircraft, requires precise maneuvers close to the aircraft operational and structural limits in specially configured aircraft. It takes years of additional training for pilots to gain the necessary skills and experience to accomplish this safely. In any case, any major change in operations as demanding as microgravity flight could well impact safety. Several NASA bodies are now in the process of reviewing the safety implications of a shift from NASA to commercial operation of the microgravity aircraft; it makes great sense to await the outcome of their studies before acting on any privatization of microgravity aircraft.

Ref: Finding #28
The team from the Langley Research Center and the Federal Aviation Administration (FAA) that produced widely applied research results on wind shear has now begun a program to study wake vortices. Like the wind shear program, the wake vortex research is designed to produce data from which operational procedures can be formulated to increase safety and more efficient terminal area operations. The first task of this effort has been to define a method for predicting the dispersion and dissipation of an aircraft's trailing vortex. This program has already begun to shed light on an important area of flight dynamics suspected of having contributed to aircraft mishaps.

Because of the importance of wake vortex research to aviation safety, the wake vortex research program should be strongly supported and, whenever meaningful data are derived, those data should be exported to the National Transportation Safety Board (NTSB), the FAA and the entire spectrum of commercial, military and general aviation.

Ref: Finding #29
Safety at the Dryden Research Center begins with the center director's personal and hands on involvement, permeates through all levels of government and contractor personnel and is codified in an outstanding *Basic Operations Manual* (BOM). Aside from the all important participation of leadership, rapid exchange of lessons learned, configuration control, design reviews, thorough flight preparation and periodic safety stand downs are only some of the elements of the Dryden program covered in the BOM. The X-31 accident investigation was extremely well done and the lessons learned therefrom immediately incorporated in the BOM.

D. OTHER

Ref: Finding #30
Fatigue and the disruption of the body's natural circadian rhythms are problems encountered when humans engage in shift work or rapidly cross time zones. Commercial pilots and shift workers are prone to the deleterious effects which include reduced performance capabilities and a resulting increase in mishap propensity. Astronauts, ground crews and the personnel who staff the Mission Control Center (MCC) often follow schedules which leave them susceptible to fatigue effects.

Researchers from NASA's Ames Research Center (ARC) and other sleep research centers worldwide have examined the impact of fatigue and circadian disruption on pilots and shift workers. The NASA group at ARC has developed a *Fatigue Countermeasures Program* which includes training and education modules which can be included in existing training programs. For example, many of the major U.S. and worldwide airlines are employing the NASA materials and are teaching them with their own instructors. Both flight and cabin crews are benefitting from receipt of the best current information on the causes of fatigue, its identification on the job, its consequences and its management.

A joint NASA, National Transportation Safety Board symposium on *Managing Fatigue in Transportation* was held on November 1-2, 1995, and attracted approximately 500 participants from multiple travel modes. There was enthusiastic support for increasing awareness of the problem and for adopting effective ways to manage fatigue through symptom identification and physiological, pharmacological, scheduling/behavioral and technological countermeasures. Additional research for an even better understanding of the problem and its remedies was also requested.

Given the proved benefits of the *Fatigue Countermeasures Program* education and training module and its widespread adoption in transportation, it would seem appropriate for the Space Shuttle and International Space Station Programs to incorporate it in existing training efforts. Astronauts, ground workers and MCC personnel could all benefit from better knowledge about the causes of fatigue and its proper management. The available materials are already designed to be adapted into existing programs without significant difficulty. The ARC is also holding regular "train the trainers" sessions to facilitate the adaptation and use of the materials.

Ref: Finding #31
The JSC *Senior Managers' Safety Course* is a two day immersion-based course which covers safety, health and environmental considerations for the senior manager. Many managers arrive at managerial level positions without any significant appreciation of what safety entails. A course such as this ensures that all managers understand the principles underlying a good safety program and helps keep them in tune with top management and its safety imperatives. This is especially important as NASA downsizes, tries to do more with less and turns to more contractor run operations. Therefore, a safety course for senior managers similar to the one conducted at JSC should be established at other NASA centers and Headquarters. Consideration should also be given to exporting the course to major NASA contractors and including it as part of both NASA and contractor managerial training.

Ref: Finding #32
NASA's ongoing reorganization and the intention to pass responsibility for Space Shuttle operations to a single Space Flight Operations Contractor (SFOC) have potential safety implications. To this point, other than an effect on morale at the KSC due to uncertainty, no significant problems have surfaced. NASA, and particularly, the Offices of Space Flight and Safety and Mission Assurance,

appear to have the Space Shuttle contracting process well in hand with safety paramount at every turn. Because of this and, possibly, because the restructuring is still in early stages, other than the aforementioned issue of KSC morale, safety problems have been few to non-existent. The cautious approach taken thus far is commendable. Nevertheless, the potential for safety problems remains. NASA leadership and top management should therefore continue active and detailed involvement in the safety aspects of planning for and oversight of NASA reorganization in general and Space Shuttle operations in particular.

Ref: Finding #33

NASA has decided to restructure and downsize its Space Shuttle operations. Many NASA personnel now working on Space Shuttle operations and sustaining engineering will be relieved of those duties. A contractor will take on an increased level of accountability and responsibility for day-to-day Space Shuttle operations. NASA will continue to have overall Space Shuttle responsibility and liability and will still be responsible for safety, flight manifest and the space flight operations budget as well as for recruiting, selecting and training crews.

As part of this plan, NASA personnel will no longer be involved in dealing with nonconformances of hardware, software and configuration requirements which are "within family." The concept is that if the task is simply to return the system to its prespecified state from a condition which has been successfully dealt with before, there is no reason for NASA to become involved. Theoretically, this is reasonable. A problem arises, however, in arriving at a suitable definition for determining if a condition is in or out-of-family and in the use of that definition on a daily basis.

The extremes of operating experience present little problem. For example, if a component or system fails which has never failed before or a serious mishap occurs, it is clearly out-of-family. Conversely, if a wear item continues to wear on every flight, that would represent an obvious in family occurrence. The problem is with many situations which fall between these extremes. Perhaps a problem which has been seen before is becoming more frequent or severe (e.g., the nozzle O-rings or the solid rocket booster pressure spikes) or one which has not been noticed for many flights suddenly starts to recur. For these types of situations, it may be extremely difficult to arrive at a definition for out-of-family which is sufficiently clear-cut. Moreover, the eventual definition of out-of-family will likely carry with it so much "overhead" that a contractor may have a strong incentive ***not*** to classify something as out-of-family whenever possible especially if the contractor bears little or no liability for an incorrect decision.

Given the importance of the definition of "out-of-family," it would seem essential for NASA personnel with direct Space Shuttle operations experience to be involved in the process of developing a definition. The derivation of the criteria for out-of-family by itself, however, will not be enough to guarantee appropriate checks and balances involving consultation with NASA. A process will have to be devised which permits NASA personnel to monitor decision-making on the status of non-conformance situations. Through this mechanism, NASA will be able to ensure that it is a part of the decision making in all situations which could potentially involve loss of crew, vehicle or significant financial resources or a major compromise to the Space Shuttle launch schedule.

Finally, the proposed future role of NASA causes a bit of a dilemma. NASA has said that it will approve all dispositions for out-of-

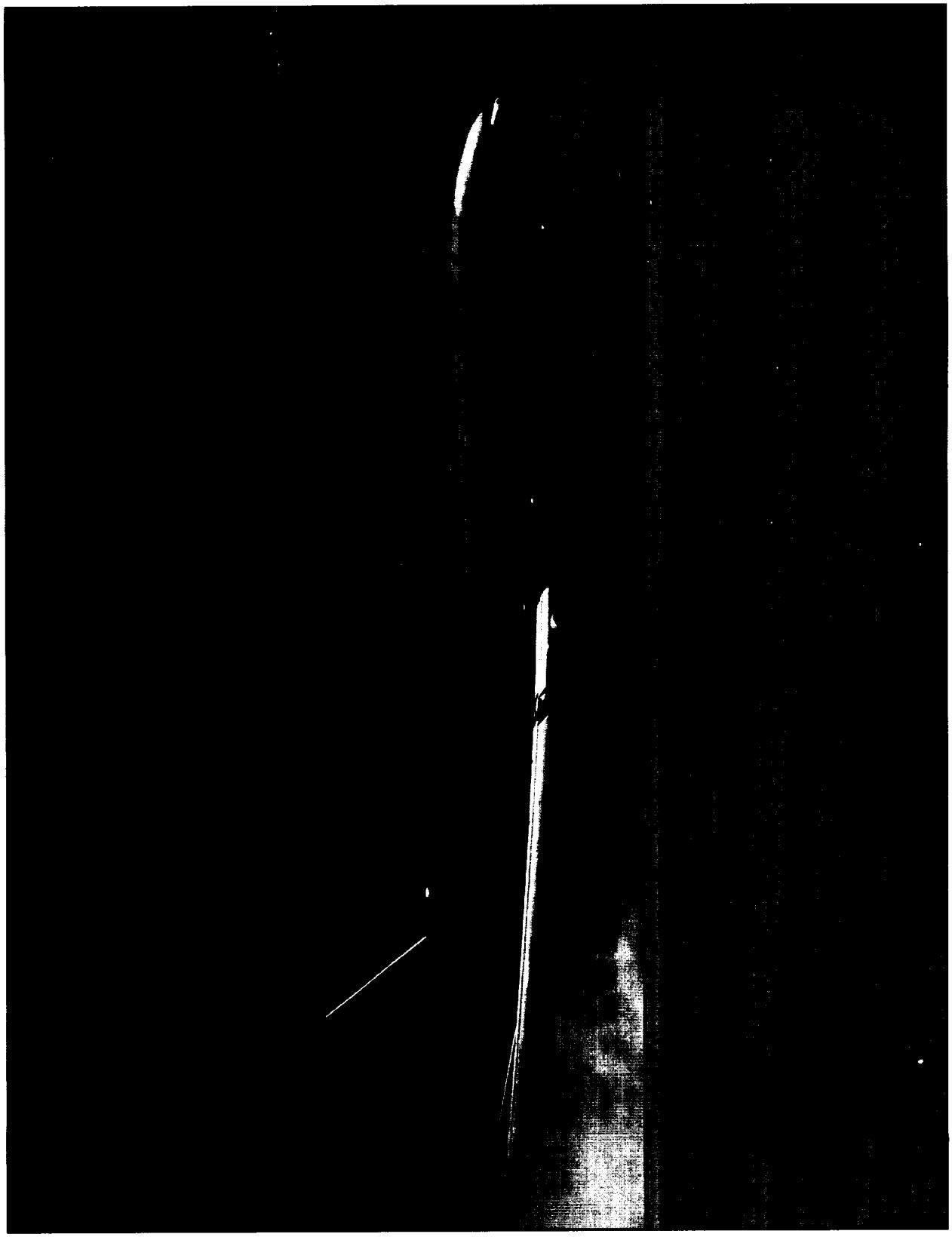
family non-conformance. With the proposed reductions of NASA personnel in operational roles, a question arises concerning what basis those in the NASA oversight role will have for making and enforcing these judgments. Initially, people can be appointed who have been involved in a "hands on" manner with the Space Shuttle. Eventually, however, NASA will run out of people with direct operational experience. At that point, the effectiveness of the NASA inputs may be compromised and safety could suffer.

Ref: Finding #34
New propulsion control modes utilizing neural nets are under development at Dryden and Ames. These allow aircraft to be reliably landed under fault conditions that previously would usually result in crashes. Neural nets are now being introduced into the Propulsion Controlled Aircraft (PCA) system. The use of neural nets in flight control systems raises questions of how this controller software can be verified and validated for flight operations. At present, they go through the standard Dryden safety processes. The first neural net experiments should not represent a Verification and Validation issue because the neural net is used on one of three redundant channels and only for capturing data.

There is ongoing work to break the neural net operation into regions each of which might be more simply validated. Nevertheless, the opinion has been expressed that there is a technology/certification mismatch at present. There is a feeling that new criteria are needed for certification for advanced control software. The Ames Research Center in its capacity as designated center of excellence for information systems technology should undertake the research and technology necessary to provide NASA with appropriate V&V techniques for neural net control software.

Ref: Finding #35
There is at least one NASA Center which has only one NASA software person in its Safety and Mission Assurance (S&MA) office to handle all of the software assurance issues. Even when a few contractor personnel are added, this is an inadequate staffing level to accomplish much meaningful assurance work on software. Moreover, the contractor personnel are not allowed to work on a number of important software evaluations because of possible proprietary conflicts. Projects seem to have developed the habit of budgeting for hardware safety analyses with little or nothing allocated for software safety. It does not seem that software safety is taken seriously! By increasing importance of software in operating systems, there is an obvious need for the S&MA organizations to penetrate more broadly throughout the Centers and provide a level of assurance commensurate with the growing role of software. Given the existence of at least one example of an under staffed software assurance function, the Headquarters Office of Safety and Mission Assurance should examine the depth of the software assurance process at each of the Centers and promulgate NASA-wide standards for adequate coverage.

IV. APPENDICES



APPENDIX A

NASA AEROSPACE SAFETY ADVISORY PANEL MEMBERSHIP

CHAIRMAN

MR. PAUL M. JOHNSTONE
Consultant, Former Senior Vice
President, Operations Services
Eastern Airlines, Inc.

DEPUTY CHAIRMAN

MR. RICHARD D. BLOMBERG
President
Dunlap and Associates, Inc.

MEMBERS

MS. YVONNE C. BRILL
Aerospace Consultant
Former Space Segment Engineer
INMARSAT

VADM ROBERT F. DUNN, USN (RET)
Aerospace Consultant/Author
Former Deputy Chief of Naval
Operations Air Warfare, Pentagon

DR. GEORGE J. GLEGHORN
Aerospace Consultant
Former Vice President & Chief Engineer
Space & Technology Group, TRW, Inc.

DR. SEYMOUR C. HIMMEL
Aerospace Consultant
Former Associate Director
NASA Lewis Research Center

DR. NORRIS J. KRONE
President
University Research Foundation

MR. NORMAN R. PARMET
Aerospace Consultant
Former Vice President, Engineering
Trans World Airlines

DR. RICHARD A. VOLZ
Head, Department of Computer Sciences
Texas A&M University

CONSULTANTS

MR. CHARLES J. DONLAN
Aerospace Consultant
Former Deputy Director
NASA Langley Research Center

MR. KENNETH G. ENGLAR
Aerospace Consultant
Former Chief Engineer, Delta Launch Vehicle
McDonnell Douglas Corporation

MR. DENNIS E. FITCH
Aerospace Consultant
Pilot
United Airlines

MR. JOHN F. MCDONALD
Former Vice President
Technical Services
TigerAir, Inc.

DR. JOHN G. STEWART
Consultant, Former Executive Director
Consortium of Research Institutions

MR. MELVIN STONE
Aerospace Consultant
Former Director of Structures
McDonnell Douglas Corporation

EX-OFFICIO MEMBER

MR. FREDERICK D. GREGORY
Associate Administrator for
Safety and Mission Assurance
NASA Headquarters

STAFF

MR. FRANK L. MANNING
Executive Director
NASA Headquarters

MS. PATRICIA M. HARMAN
Staff Assistant
NASA Headquarters

APPENDIX B
NASA RESPONSE TO MARCH 1995 ANNUAL REPORT

SUMMARY

NASA responded on July 14, 1995, to the "Findings and Recommendations" from the March 1995 Annual Report. NASA's response to each report item is categorized by the Panel as "open, continuing, or closed." Open items are those on which the Panel differs with the NASA response in one or more respects. They are typically addressed by a new finding and recommendation in this report. Continuing items involve concerns that are an inherent part of NASA operations or have not progressed sufficiently to permit a final determination by the Panel. These will remain a focus of the Panel's activities during the next year. Items considered answered adequately are deemed closed.

Based on the Panel's review of the NASA response and the information gathered during the 1995 period, the Panel considers that the following is the status of the recommendations made in the 1995 report.

	RECOMMENDATION	
NUMBER	SUBJECT	STATUS
1	International Space Station (ISS) Independent Safety Assessment Function	CONTINUING
2	ISS Assured Crew Return Capability	OPEN
3	ISS Caution and Warning	OPEN
4	ISS Fire Suppression Effectiveness	OPEN
5	ISS Hazardous Materials and Procedures	CLOSED
6	ISS Orbital Debris Protection	OPEN
7	Russian Androgynous Peripheral Docking System (APDS) Hook Capture Indicator	CLOSED
8	APDS Backup Systems - Pyro Bolts	OPEN
9	Additional Space Shuttle Payload Capability	CLOSED
10	New Gas Generator Valve Module	CLOSED
11	Advanced Orbiter Displays/System Working Group	OPEN
12	Tactical Air Control & Navigation/Microwave Scanning Beam Landing System Obsolescence	CONTINUING
13	Data Processing Requirements Growth	OPEN
14	Improve Autoland Equipment and Crew Flight Rules and Training	CLOSED
15	Space Shuttle Main Engines (SSME) Inspection and Assembly Processes	CONTINUING
16	SSME Block II Modifications	CLOSED
17	SSME Health Monitoring	CONTINUING
18	SSME Block II Safety Improvement	OPEN
19	Super Lightweight Tank Ultimate Loads Test	CLOSED
20	Solid Rocket Booster Structural Tests	CLOSED
21	Critical Components Cannibalization	CLOSED
22	Integrated Logistics Panel	CLOSED
23	KSC Logistics Consolidation Plan	CLOSED
24	TU-144 Design and Safety Assessment	CLOSED
25	Wind Shear Research	OPEN
26	Tire Research Program	OPEN
27	Propulsion Controlled Aircraft System	CLOSED
28	Unmanned Aerial Vehicle Range Safety Policy	CLOSED
29	Simplified Aid for EVA Rescue	OPEN
30	Priority of Software Issues	CONTINUING
31	Independent Safety Oversight of Human Experiments	CLOSED
32	Aviation Safety Reporting System	CLOSED
33	Aircraft Operations Specialists Advisory Group	CLOSED
34	Total Quality Management	CLOSED

National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001

JUL 14 1995

Mr. Paul M. Johnstone
Chairman, Aerospace Safety
Advisory Panel
24181 Old House Cove Road
St. Michaels, MD 21663

Dear Mr. Johnstone:

In accordance with Mr. Norman R. Parmet's introductory letter to the March 1995 Aerospace Safety Advisory Panel (ASAP) Annual Report, enclosed is NASA's detailed response to Section II, "Findings and Recommendations."

The ASAP's efforts in assisting NASA in maintaining the highest possible safety standards are commendable. Your recommendations are highly regarded and play an important role in risk reduction in NASA programs.

We thank you and your Panel members for your valuable contributions. ASAP recommendations receive the full attention of NASA senior management. We look forward to working with you.

Sincerely,

Daniel S. Goldin
Administrator

Enclosure

1995 AEROSPACE SAFETY ADVISORY PANEL REPORT

FINDINGS, RECOMMENDATIONS, AND RESPONSES

A. SPACE STATION PROGRAM

Finding #1:
The original organization of the International Space Station (ISS) Program included an independent safety assessment function reporting directly to the Program Manager. Subsequently, this was changed so that independent assessment reported directly to the Associate Administrator for Safety and Mission Assurance.

Recommendation #1:
Maintain the true independence of the safety assessment function by ensuring that it reports outside the Space Station Program.

NASA Response to Recommendation #1:
NASA agrees. The International Space Station Independent Assessment Team (IAT) reports directly to the Office of Safety and Mission Assurance (S&MA) at NASA Headquarters. At the same time, the S&MA team within the Space Station program provides early and continuous S&MA input to design and operations, allowing for efficient incorporation and implementation of the requirements. This is in addition to maintaining a reporting path to the IAT.

Finding #2:
The ISS Program has committed to providing an assured crew return capability. This will initially be accomplished by using a combination of docked Space Shuttles and Soyuz capsules. Once the ISS is permanently and fully staffed, a newly designed Assured Crew Return Vehicle (ACRV) will be deployed.

Recommendation #2:
The use of the Space Shuttle and Soyuz as an interim measure [for assured crew return] is an expedient. The planned new ACRV is definitely needed to support safety in the long term. The design of this permanent ACRV, regardless of where and when it is built, should be consistent with the design reference missions and systems requirements previously defined by the ACRV Office of the Space Station Freedom.

NASA Response to Recommendation #2:
NASA agrees. The ACRV documentation presently in place in the Space Station program (SSP 41000A and 50011-01 Rev A) is consistent with the design reference missions and systems requirements previously defined by the ACRV Office of the Space Station Freedom.

Finding #3:
The architecture of the ISS contains a Caution and Warning (C&W) system to detect and warn of malfunctions and emergencies, including toxic spills, depressurization and fire. The system makes use of laptop computers for localization of faults.

Recommendation #3:
Careful consideration should be given to the appropriateness of using laptop computers for a task as time critical as localizing life-threatening emergencies. The entire fault detection and localization process should use dedicated equipment to minimize response time.

NASA Response to Recommendation #3:
To address this issue, NASA has formed a temporary team, composed of personnel from Safety and Mission Assurance, Command and Data Handling, and other teams. Program resolution of these issues is expected by August 1995.

Finding #4:
The absence of experimental data for fire suppression effectiveness of the carbon dioxide extinguishers selected for use on the ISS under weightless conditions is a source of concern.

Recommendation #4:
Appropriate ground-based and in-flight research to confirm the suitability of the use of pressurized carbon dioxide fire extinguishers under weightlessness should be conducted.

NASA Response to Recommendation #4:
Ground testing performed during the Space Station Freedom program conservatively demonstrated the ability of the carbon dioxide fire extinguishers to produce adequate concentrations of fire suppressant in closed volumes, such as racks. Additional ground testing is being pursued to address areas, such as endcones and standoffs, not included in the Freedom configurations tested. Upon successful demonstration that these new configurations do not exceed the capabilities of the extinguishers to adequately perform, NASA will consider them to be suitable for use on the Space Station.

Finding #5:
The present procedures for monitoring or controlling hazardous materials and procedures used in ISS experiments are dependent on the experiment supplier complying with Station requirements and specifications.

Recommendation #5:
For hazardous materials and procedures used in Space Station experiments, NASA should establish a positive system of compliance assurance modeled after the one used by the Space Shuttle Program. This system should consider the entire service life of the experiment and its deactivation when completed.

NASA Response to Recommendation #5:
NASA agrees with and is complying with this recommendation. The Space Station program is using the same Payload Safety Review Panel (PSRP) that the Space Shuttle program is using, augmented with representatives from the Space Station program and the international partners. The PSRP process document has been levied on the Space Station program, as has the payload safety requirements document with a Station-specific addendum to cover the differing environments.

Finding #6:
Good progress has been made in defining the threat from orbital debris and in demonstrating efficient shielding configurations. A technical basis for a debris protection specification for ISS is emerging.

Recommendation #6:
Continue [orbital debris protection] design with emphasis on: structural integrity of habitable modules and pressure vessels; identification of the damage potential from direct impact and other depressurization events; and definition and development of operational procedures and policies.

NASA Response to Recommendation #6:
NASA shares the ASAP's areas of concern related to orbital debris. The Space Station program continues to place emphasis on the integrity of habitable modules and pressure vessels. As previously reported to the ASAP, we have implemented state-of-the-art enhanced shielding on the U.S. Laboratory and Habitation modules. Similar approaches are being taken by the international partners to meet Space Station requirements. We are also continuing efforts to identify damage potential from debris with ongoing penetration effects analysis and test activities at the Marshall Space Flight Center. Operational procedures and policies for risk mitigation are under development. Techniques for executing collision avoidance maneuvers are maturing and other activities, including penetration detection and repair, are ongoing.

B. SHUTTLE/MIR (PHASE ONE) PROGRAM

Finding #7:
The Russian Androgynous Peripheral Docking System (APDS) for docking the Space Shuttle with the Mir uses 12 active hooks on the Space Shuttle side which mate with an equal number of passive hooks on the Mir. The design currently provides no positive means of determining whether any or all of the hooks are secured. NASA has decided it is an acceptable risk to fly the first docking mission, STS-71, without an indicator.

Recommendation #7:
NASA should develop an indicator system.

NASA Response to Recommendation #7:
The second APDS unit, which is being procured from RSC-Energia for the second and subsequent Mir missions, also does not have individual structural hook position indicators. The addition of indicators was discussed with RSC-Energia, however, the APDS manufacturing and delivery schedule precluded installation. Johnson Space Center (JSC) and Rockwell engineers have shown, through test and analysis, that there is no threat to crew and vehicle safety for the remote failure case of two adjacent hooks failing to close properly. Combinations of failures that would result in crew injury or vehicle damage are considered to be of remote probability, the risk therefore being acceptable for the Phase I program. The Shuttle program has reviewed the test and analysis results and approved the APDS baseline without position indicators for the Mir missions.

The design specification for APDS units which will be procured from RSC-Energia for international Space Station mission applications currently requires position indication capability for all structural hooks on the orbiter (active) side of the interface, and position indication for gangs of three structural hooks on the station (passive) side. In addition, the APDS which will be installed on the Pressurized Mating Adapter-1, and controlled from the orbiter on Space Station Mission-2A, will have positive indications on all structural hooks.

Finding #8:
If the primary system fails, the first backup separation system for the APDS is a set of pyro bolts which disengage the 12 active hooks. Having to rely on the pyros as presently supplied by the Russian Space Agency poses risk because of lack of knowledge relating to the pyros' pedigree and certification. A second contingency demate procedure is available involving the Extravehicular Activity (EVA) removal of 96 bolts at a different interface. Implementing either backup method to separate Shuttle from Mir may leave the Mir port unusable for future dockings.

Recommendation #8:
NASA should emphasize increasing the reliability of the primary mating/demating mechanisms in order to reduce the likelihood of having to use either of the backups. NASA should also obtain an acceptable certification of the supplied pyro bolts. Failing that, NASA should procure fully certified substitute bolts.

NASA Response to Recommendation #8:
The APDS mechanism hardware has been demonstrated by test to fully meet its design environments. Additional detail regarding critical mechanical components was jointly developed by RSC-Energia, JSC, and Rockwell engineering, and analysis of those components has been completed. The analysis supports test results which demonstrate design margin for the life of the Mir program. Additionally, the results for this analysis will be used as a guideline in developing maintenance requirements for future Mir and Station missions. The pyrotechnics, installed in the APDS, have completed a confidence test that was developed by Rockwell and NASA engineering in conjunction with RSC-Energia and with the concurrence of NASA S&MA. NASA is pursuing design improvements of the RSC-Energia bolts for Station missions and is also working on the development of an American-built pyrotechnic bolt.
RSC-Energia has not been receptive to the idea of installing American bolts in the APDS; however, assembly schedules do not require a decision until late 1995, and discussions with RSC-Energia are continuing.

C. SPACE SHUTTLE PROGRAM

ORBITOR

Finding #9:
Significant additional payload mass capability is required to meet the demands of the assembly and supply plans. Much of the needed increase in capacity will be achieved through weight reduction programs on a number of Space Shuttle elements and subsystems. The large number

of simultaneous changes creates potential tracking and communication problems among system managers.

Recommendation #9:
Emphasis should be placed on the adequate integration of all of the changes into the total system.

NASA Response to Recommendation #9:
Integration of major changes into the existing Space Shuttle vehicle is receiving emphasis by the Space Shuttle program. The Space Shuttle program has had a system in place for many years to integrate all of the changes into the total system. This system has proven effective.

The system consists of technical panels, integrated product teams, and control boards. A technical panel exists for each major functional area (e.g., Loads and Dynamics, Thermal). These technical panels integrate and review the technical aspects of the analysis and testing. The functional areas are integrated by the integrated product teams (e.g., Propulsion System Integration Group) and at joint panel meetings.

The control boards, at the project and program level, provide a final technical review and integration, and management direction for cost and schedule control.

The NASA Element Project Offices and prime contractors are represented on the technical panels, integrated product teams, and control boards, allowing cross communication and input at all levels of the process.

There is a System Integration Plan for each of the major performance enhancements that defines the responsibilities of the affected elements, identifies deliverable products and hardware, and defines the system schedule for that enhancement to support the first element launch.

Finding #10:
The New Gas Generator Valve Module (NGGVM), when certified and retrofitted to the fleet, should mitigate many of the problems with the current Improved Gas Generator Valve Module in the Improved Auxiliary Power Unit (IAPU). The NGGVM development program is proceeding well.

Recommendation #10:
NASA should attempt to introduce the NGGVM into the fleet as soon as possible as a safety and logistics improvement.

NASA Response to Recommendation #10:
NASA intends to introduce the NGGVM into the fleet on an opportunity basis. The ground rule for this plan is to maintain a minimum Kennedy Space Center (KSC) stock level of five spare IAPU's to support any unplanned line replaceable unit removals. Any other IAPU's not required to support this stock level will be shipped to Sundstrand to undergo the NGGVM modification. By leaving this number of spare IAPU's on the shelf at KSC and modifying any units available

beyond that, the NGGVM implementation into the fleet can be completed in late 1998 or early 1999. Upgrade and modification of three Auxiliary Power Units currently not used for flight as an expedient to the NGGVM fleet retrofit is not cost effective.

Finding #11:
The decision has been made to install the entire Multi-Function Electronic Display System (MEDS) in each Orbiter during a single Orbiter Maintenance and Down Period (OMDP). An Advanced Orbiter Displays/System Working Group has been formed to plan for the next generation of MEDS formats and display enhancements.

Recommendation #11:
NASA should support the Advanced Orbiter Displays/System Working Group and set a timetable for the introduction of enhanced display
formats which will improve both safety and operability. It should also maintain its commitment to completing the MEDS installations during a single OMDP.

NASA Response to Recommendation #11:
NASA established the Advanced Orbiter Displays/System Working Group to define next-generation cockpit displays that will take advantage of MEDS data processing capabilities to improve safety and operability. The Government/industry working group is currently defining requirements for enhanced displays as well as a timetable for both evaluation of candidate displays in MEDS testbeds and introduction of new displays into orbiters.

NASA identified several advantages to installing MEDS hardware in orbiters during a single OMDP. Current OMDP planning as well as the schedule for first flight of MEDS on each orbiter reflects the single OMDP installation plan.

Finding #12:
The Tactical Air Control and Navigation (TACAN) and Microwave Scanning Beam Landing System (MSBLS) on-board receivers are obsolescent and increasingly difficult to maintain. The MSBLS receivers also have known design problems which can lead to erroneous guidance information if the orbiter is operating with only two of the three receiver complement. A Global Positioning System (GPS) test is underway on one of the orbiters using the backup flight software and computer. The use of GPS could replace both the TACAN and MSBLS systems as well as assisting ascent and on-orbit operations.

Recommendation #12:
Given the potential of GPS to improve safety and reliability, reduce weight and avoid obsolescence and the many existing and potential problems with the use of TACAN and MSBLS, a full GPS implementation on the orbiter should be accomplished as soon as possible.

NASA Response to Recommendation #12:
The Space Shuttle program is currently reviewing a plan to fully implement the GPS capabilities. The GPS hardware/software implementation plan calls for completing the installation of a redundant GPS hardware capability as early as the year 2000. The software implementation will be completed with delivery of the OI-27 operational increment by December 1997 with a first

flight effectivity in the summer of 1998. The redundant GPS hardware installation will be accomplished during the OMDP for each orbiter.

Finding #13:
Growth in the requirements for on-board data processing will continue as the Space Shuttle is used in support of Shuttle/Mir, ISS and other future missions. The length of time over which the General Purpose Computer and its software will be able to meet these growing needs effectively is likely inadequate.

Recommendation #13:
NASA should expedite a long-range strategic hardware and software planning effort to identify ways to supply future computational needs of the Space Shuttle throughout its lifetime. Postponing this activity invites a critical situation in the future.

NASA Response to Recommendation #13:
We concur that continued reliance on the Space Shuttle beyond 2005 will demand some major revisions to the core General Purpose Computer (GPC) hardware and software, if for no other reason than the inability to maintain hardware based on early 1980 technology. Such a revision, given the tightly coupled interdependencies of the present core architecture, would logically be accomplished as a major "block" update rather than gradually evolving to a new architecture. The block update approach can also serve to reduce future operations costs by stabilizing avionics hardware and software during the Station assembly era. In accord with that concept, the Space Shuttle program is considering an approach that would freeze the GPC software at roughly the turn of the century, following the incorporation of Station-driven enhancements. That freeze would allow for diversion of engineering resources, heretofore devoted to routinely evolving enhancements, to pursue a true significant block update sufficient to sustain the Space Shuttle past 2020.

As the foundation for such a possible architecture, the JSC Engineering Directorate has developed a Reduced Instruction Set Computer (RISC) for high-fidelity emulation of the present GPC. That emulation is capable of real-time bit-level execution of actual object code produced by the HAL/S compiler. It will soon be made available to allow flight software developers a target machine for early development testing. At the present time, such early testing is a premium because of the limited availability of real GPC's. The extension of the emulator concept, as a candidate to replace the actual flight GPC's, is the next logical step. It would preserve critical flight code, thereby minimizing the reverification costs, while still providing a modern platform for growth.

In summary, NASA does have the essential formative elements for a long-range strategic hardware and software upgrade effort in work. Existing limited resources and ongoing program activities obviously preclude any definitive strategic planning until completion of the current programwide restructuring activities. Once those activities are complete, a more definitive plan and schedule, predicated on critical examination of limited available resources, can be developed.

Finding #14:
The STS-64 mission involved a higher than usual level of windshield hazing which could have led to a situation in which the astronauts' view of the landing runway was obscured. MSBLS and TACAN are obsolescent. There is also the possibility that false indications by MSBLS under certain scenarios could result in an unacceptable risk of a landing mishap. Thus there is a clear need for early upgrade of orbiter and support facility autoland equipment and crew flight rules and training improvement.

Recommendation #14:
NASA should improve the autoland equipment on the Orbiter; for example, replacing MSBLS and TACAN with GPS. In the interim, NASA should ensure that operations and failure modes of MSBLS are fully examined and understood. NASA should also reexamine the training of crews for executing automatic landings, including autoland system familiarization. Astronaut commanders and pilots should discuss circumstances which might warrant autoland use prior to each mission and be prepared for all reasonable contingencies in its operation.

NASA Response to Recommendation #14:
Incorporation of GPS is being pursued as aggressively as funding and technical constraints will allow. The program has approved plans and funding to provide a single-string GPS capability that can be flown in the summer of 1997 as a first step toward TACAN/MSBLS replacement. Plans for a full three-string operational system have been approved for OI-27, and detailed costs and schedules are being assessed by the program. The failure modes of the MSBLS have been analyzed and are documented in the program's Critical Item List.

The finding made by the ASAP regarding the STS-64 mission, involving a higher than usual level of windshield hazing that could have led to a situation in which the astronaut's view of the landing runway was obscured, is incorrect. The STS-64 orbiter Quick Look Reports states: "Orbiter Windows 3 and 4 exhibited light hazing and streaks were seen on 4." Additionally, the Commander (Richard N. Richards, 4th flight) reports that the window hazing was not unusual at all, typical of what is usually seen, and an excellent view of the runway was obtained at all times during the approach, landing, and rollout phases of the flight. The STS-64 vehicle touchdown parameters were excellent, confirming that the Commander had an excellent view of all visual aids throughout the approach and landing. (These touchdown parameters include touchdown airspeed of 198 knots versus 195 planned, touchdown distance of 2386 feet versus predicted 2505, sink rate at touchdown of 1.0 feet per second, and a threshold crossing height of 20 feet. All parameters are excellent.)

Extensive analysis of the orbiter autoland system has been performed by various organizations in NASA, including exhaustive reviews by NASA Safety and Mission Assurance personnel. Those results have been briefed to all levels of NASA management. The Space Shuttle program has not identified/defined any hardware or software change that is necessary to improve the autoland capability. The operational use of the autoland capability remains at the discretion of the mission commander. To educate pilots and commanders on the use of this emergency system, Mission Operations Directorate (MOD) provides a briefing that covers the capabilities and limitations of the autoland system, as well as the contingency cases for which it is a viable alternative (i.e., both pilots incapacitated, or a highly inaccurate weather forecast for landing). In

addition, each crew has a session in the Shuttle Mission Simulator, as well as the Shuttle Training Aircraft where the autoland system is demonstrated and discussed.

SPACE SHUTTLE MAIN ENGINE (SSME)

Finding #15:
It has become necessary to execute a partial disassembly of both the engines and turbopumps after each flight because of the accumulation of special inspection requirements and service life limits on components of the current (Phase II) SSMEs. These inspections are performed with rigor and appropriate attention to detail.

Recommendation #15:
In order to control risk, NASA must maintain the present level of strict discipline and attention to detail in carrying out inspection and assembly processes to ensure the reliability and safety of the SSMEs even after the Block I and Block II upgrades are introduced.

NASA Response to Recommendation #15:
NASA agrees with this recommendation and will continue to perform the detailed inspections of the Phase II Space Shuttle Main Engines (SSME) that are currently defined. The postflight inspections of both the Block I and Block II SSME's will be significantly less in frequency than those for today's Phase II SSME due to the major design changes, especially in the turbopumps. However, the program plans to use the same level of strict discipline and attention to detail in carrying out the new inspection program as it has in the past.

Finding #16:
The re-start of the Advanced Turbopump Program (ATP) High Pressure Fuel Turbopump (HPFTP) and the start of the Large Throat Main Combustion Chamber (LTMCC) developments were authorized in the spring of 1994. Combined with the ongoing component developments of the Block I engine, this will produce a Block II engine which will contain all of the major component improvements that have been recommended over the past decade to enhance the safety and reliability of the SSME. Both the Block I and Block II programs have made excellent progress during the current year and are meeting their technical objectives.

Recommendation #16:
Continue the development of the Block II modifications for introduction at the earliest possible time.

NASA Response to Recommendation #16:
NASA agrees with this recommendation. The first flight of the Block I SSME was on STS-70, which was launched on July 13, 1995. The Block II SSME will be available for flight in September 1997.

Finding #17:
In order to provide an engine health monitoring system that can significantly enhance the safety of the SSME, improvements must be made in the reliability of the engine sensors and the computational capacity of the controller. It is also essential to eliminate the difficulties with the

cables and connectors of the Flight Accelerometer Safety Cut-Off System (FASCOS) so that vibration data can be included in the parameters used in the algorithms that determine engine health.

Recommendation #17:
Expand and emphasize the program to improve engine health monitoring. Continue the program of sensor improvements. Vigorously address and solve the cable and connector problems that exist in FASCOS. Continue the development of health monitoring algorithms which reduce false alarms and increase the detectability of true failures.

NASA Response to Recommendation #17:
The Space Shuttle program is implementing Discharge Temperature Thermocouples as a replacement for the current temperature sensors on the SSME's. No other health monitoring improvements are funded at this time because the design was not mature enough to make this a cost-effective project.

Finding #18:
The Block II SSME can improve safety if an abort is required because it can be operated more confidently at a higher thrust level. This will permit greater flexibility in the selection among abort modes.

Recommendation #18:
NASA should reexamine the relative risks of the various abort types given the projected operating characteristics of the Block II SSMEs. Particular emphasis should be placed on the possibility of eliminating or significantly reducing exposure to a Return to Launch Site abort.

NASA Response to Recommendation #18:
Operating the Block II SSME's at a higher power level requires completion of two certification activities—the Block II SSME hardware certification and the integrated vehicle intact abort certification (loads, thermal, guidance, navigation and control). Because the internal environments and stresses are significantly reduced for Block II SSME's, the Space Shuttle program approved certification testing to include 109-percent power level for intact abort operations. This allows for the future consideration of increasing the power level for intact aborts to 109 percent pending the results of certification testing. If the increase in power level for intact aborts proves feasible, it would reduce, but not eliminate, exposure to the Return-to-Launch Site abort mode. Performance enhancements vehicle ascent certification environments are currently being developed using 106-percent power level for intact abort operations to improve abort performance and to minimize the risk of design impacts to the Space Shuttle vehicle. A delta certification plan to incorporate 109-percent power level for intact abort operations is currently being developed. Implementation of the plan is contingent on a successful Block II SSME test program, the results of vehicle thermal and structural loads trade studies, and the delta certification cost and schedule. Further, even if certification is successful, the decision to utilize 109-percent power level for intact aborts will depend on actual flight experience with the Block II SSME's.

EXTERNAL TANK

Finding #19:
The liquid oxygen tank aft dome gore panel thickness of the Super Lightweight Tank (SLWT) has been reduced significantly on the basis of analyses. To stiffen the dome, a rib was added. The current plan to verify the strength of the aft dome involves a proof test only to limit load. Buckling phenomena cannot be extrapolated with confidence between limit and ultimate loads.

Recommendation #19:
The SLWT aft dome should either be tested to ultimate loads or its strength should be increased to account for the uncertainties in extrapolation.

NASA Response to Recommendation #19:
NASA agrees with this recommendation. At the joint NASA and Martin Marietta Aluminum Lithium Test Article (ALTA) Design Review on August 19, 1994, an aft LO2 dome test was added to the ALTA test program. Adding this stability test will permit the aft dome to be verified to the ultimate load condition. The as-planned test satisfies the buckling concerns of Finding #19.

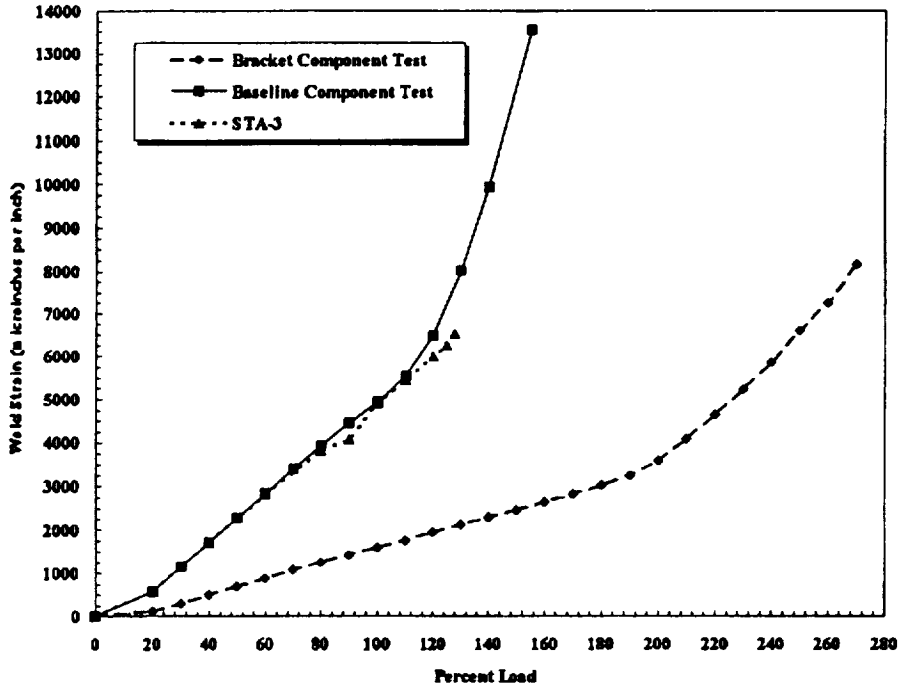
SOLID ROCKET BOOSTER (SRB)

Finding #20:
The structural tests of a segment of an SRB aft skirt in the baseline configuration did not duplicate the strains and stresses previously measured in the tests of the full-scale aft skirt Structural Test Article (STA-3). This suggests that segment testing of the proposed bracket modification to improve the aft skirt's factor of safety may not be valid.

Recommendation #20:
NASA should reassess the use of the segment test method and reconsider the use of a full scale test article for qualifying the proposed bracket reinforcement.

NASA Response to Recommendation #20:
At the time of the NASA response to the March 1994 ASAP Annual Report, two initial test condition baselining test articles (TA) had been tested to 100- and 70-percent load levels. The TA-1 and TA-3 test loads were analytically derived and validated using empirical data from these tests and STA-3. The TA-3 baseline testing showed excellent correlation with strain response curves measured during the STA-3 test. In addition, a second test article was tested to failure. Strain data obtained from these two specimens was compared to the STA-3 strain data (up to 128-percent loads which was the maximum load level achieved prior to failure initiation during the STA-3 test program). Data from second baseline test, the bracket test, and STA-3 are depicted in the figure below. The strain measurements for the critical weld region for the full-load applications (0 to 128-percent loads) exhibit an average correlation within 8.6 percent and, at 128-percent load levels, the average correlation is within 9.6 percent.

The first of the two test articles that were tested to failure failed at 167-percent load level; the second at 155-percent load level. The corresponding strains at the indicator gage at failure were ~17,000 and ~13,500 microstrain; by comparison, the STA-3 measurements indicated 6,704 microstrain at 128-percent load level (the level of failure). It was also noted that STA-2B, a skirt test for the filament wound case program tested in 1986, failed at 10,708 microstrain at 129-percent load level. Comparison of the test results indicates variability exists in the failure strains at the critical gage locations. The apparent disparity was investigated by NASA using a fault-tree methodology. Although no specific cause has been identified for this variability, the following items are probable contributors:



- Material property variation between the test articles.
- Residual stresses resulting from assembly, welding, and/or previous use.
- Other skirt-to-skirt variation; geometry, tolerances and strain-gage location.
- Component test not accurately representing the full-skirt configuration.
- An unidentified contributor.
- A combination of the above factors.

Following this investigation, the cost/benefit of proceeding with the test team investigation versus ending the effort was evaluated and the investigation terminated. The following rationale supported this decision.

The test program also included testing with a bracketed test article. The article was tested to the limits of the test support structure (270-percent load level) without a weld failure occurring. A comparison between the two test configurations (with and without the bracket) demonstrated a minimum increase in capability of the bracketed skirt section of 62 percent. This indicates that

the addition of the external bracket would return the aft skirt critical weld factor of safety to a value in excess of 2.0. The two tests, performed in the same manner and test configuration, should allow comparable quantitative evaluation of performance. The 62-percent increase in capability mitigates significantly any concerns with the minor variations (<10 percent) in strain levels between component test articles and STA-3 up to 128 percent, and those variations in load capability measured during the entirety of the test series.

The pedigree of flight hardware is assessed following each flight and a statistical pedigree has been established. Evaluation of skirts, following 67 successful launches plus Flight Readiness Firings and pad aborts, has identified no deterioration of the welds as a result of flight loads.

STA-3 sustained 100-percent load for both prelaunch and rebound cases. The initial weld failure occurred at 128 percent with sufficient structural redundancy to allow continued loading to 142 percent. The skirt reacted loads were greater than the design limit for more than 7 minutes after the initial failure.

The flight hardware assessment and loading includes the following:

a. The Mobile Launch Platform (MLP) spherical bearings are now biased radially inward to ensure favorable assembly conditions exist. The support post bushings/bearings have been locked to preclude the undesirable effects of load slip.

b. Each skirt has been instrumented (only one has yet to be included in this data base) to measure the system strains. This has resulted in 52 sets of full-scale strain data from 27 flights. The data correspond well with STA-3 and the component testing. The average peak strain during the SSME thrust buildup is 4181 microstrain with a standard deviation of 381 microstrain. The maximum measured strain was 5072 microstrain (excluding STS-44, S/N 20029 which recorded an apparent strain level of 5488 microstrain due to the Bauschinger effect). The comparable strain from the test programs (including STA-3) at 100-percent load was approximately 5080 microstrain.

c. Variation in on-pad loads, as indicated by MLP instrumentation and verified by the aft skirt strain gage data, is small.

In summary, component test results indicate that the external bracket significantly enhances critical weld factors of safety. In addition to providing substantive quantitative verification of existing analytical techniques, the completed evaluation of the test program results has provided no challenge to or indictment of current flight rationale. The resultant potential benefits from introduction of the bracket are limited. The design change has minimal potential for increasing the Shuttle lift-off wind allowables (and associated probability of launch), as other elements are similarly constraining. The elimination of the Advanced Solid Rocket Motor effort precludes near-term concerns for substantially increased skirt loading. The significant component, subscale and

full-scale analysis and test, along with individualized measurements of each aft skirt, provide a level of understanding such that no further concerns exist for a demonstrated 1.28 factor of safety in the critical weld area. Therefore, implementation of the bracket is not planned at this time, and the program plans to change the appropriate specification requirement to reflect this factor of safety to avoid repetitive flight-by-flight waivers.

LOGISTICS AND SUPPORT

Finding #21:
The effort by the NASA logistics organization and its principal contractors has resulted in satisfactory performance. There remain a few problems, such as a tendency towards increased cannibalization, which still require attention.

Recommendation #21:
Every effort should be made to avoid cannibalizations, particularly on critical components such as the SSME and the IAPU.

NASA Response to Recommendation #21:
While there were some increases in cannibalizations in mid-1994, continued management attention has maintained an overall decreasing trend in cannibalizations. Close attention to related indicators will continue. There are currently four spare IAPU's on the shelf at KSC. No IAPU cannibalizations have occurred since 1993.

Finding #22:
The Integrated Logistics Panel (ILP) continues to meet at six-month intervals, usually at the Kennedy Space Center (KSC) or the Marshall Space Flight Center. The ILP serves a valuable coordinating and liaison function for the entire logistics operation. Its personnel complement has been reduced as part of the overall NASA staff cutbacks.

Recommendation #22:
NASA should maintain support of an effective ILP.

NASA Response to Recommendation #22:
Space Shuttle program and project elements continue to support the ILP and related integration activities. Even though personnel cutbacks have been experienced, the ILP is still an effective forum for problem solving, lessons learned, and technical information exchange. In addition, the prime contractors continue to benefit from the exchange of technical data presented at these meetings.

Finding #23:
There is a plan to consolidate all logistics elements at KSC except Spacelab over the next three or four years. This should unify the entire logistics and supply organization. The realignments are intended to eliminate duplication of effort, gain efficiency in support and materially reduce the cost of operation.

Recommendation #23:
Proceed as outlined in the NASA plan.

NASA Response to Recommendation #23:
A single organization consolidating all KSC logistics elements was officially established on April 17, 1995. This new organization integrates logistics functions from the Payload Management and Operations Directorate, the Installation Management and Operations Directorate, the Engineering Development Directorate, and the Shuttle Management and Operations Directorate. This new organization, known as the Logistics Operations Directorate, is now proceeding with internal realignments to eliminate duplication, increase efficiency, and reduce costs while improving customer service.

D. AERONAUTICS

Finding #24:
NASA has entered into a contract with the Tupolev Design Bureau of Russia to support flights of a TU-144 supersonic airplane for a joint U.S./Russian research program. The TU-144 has a questionable safety record, and the particular airplane to be used has not been flown for a number of years. The level of assurance available for this flight project may not be equivalent to that typically associated with NASA's flight research programs.

Recommendation #24:
NASA should assure that all design and safety data and operational characteristics of this vehicle have been fully explored.

NASA Response to Recommendation #24:
The TU-144 Supersonic Flight Research program was developed in consonance with the Gore/Chernomyrdin Agreement on Aeronautics Cooperation of June 1993. The TU-144, as a supersonic testbed aircraft, provides an opportunity to obtain in-flight measurements of information pertinent to future development of a High-Speed Civil Transport aircraft. Given this opportunity, the U.S. aircraft manufacturing industry encouraged NASA, as part of its High Speed Research (HSR) program, to institute an effort that would return a TU-144 aircraft to flight status and conduct a series of flight experiments on the upgraded and instrumented aircraft. A NASA/U.S. industry team has been formulated to lead the effort that will result in the aircraft being returned to a flight status for the completion of six flight experiments.

Prior to contracting for the aircraft refurbishment and instrumentation, a detailed feasibility study was conducted and reported to NASA in December 1993 by Rockwell International Corporation. Also, a series of ground tests and subsystem checkouts were conducted by Tupolev in February 1994 on the aircraft to be upgraded. These tests exercised fuel, hydraulic, and avionics systems and identified line replaceable units that would need to be modified, refurbished, or replaced. TU-144 design and operations data were delivered to the U.S. team as part

of these studies and tests. Given favorable results from these feasibility assessments, a contract for the aircraft modification and instrumentation was awarded in August 1994. These program phases are currently in progress. Boeing is the lead U.S. contractor (with McDonnell Douglas sharing a partnership role) and Rockwell International is a subcontractor with responsibility for oversight of aircraft modifications performed by Tupolev.

As part of the aircraft modification phase, the U.S. team requested and was provided with detailed design and safety data required to ensure mission safety and success. In addition, mission planning and flight manifest determinations are being conducted concurrently with the aircraft modification. Tupolev has provided detailed operational data and characteristics obtained during initial TU-144 flight testing. Tupolev and NASA engineers are actively involved in the mission planning activities. Rockwell has hired a full-time engineer at their permanent office in Moscow who serves as an onsite representative at Tupolev and provides regular status reports to the U.S. team. The Rockwell representative has many years of experience in Russian aviation as an employee of the Gromov Flight Research Institute and the Kamov Helicopter Company. He is very knowledgeable about the Russian aircraft industry and the Russian airworthiness process.

Given the international nature of the program and the fact that all of the flights to be conducted under this program will be flown in Russia, it was understood that Russian airworthiness and certification procedures would be utilized to ensure airworthiness of the aircraft. The U.S. industry/NASA TU-144 project team concerned with airworthiness has spent significant effort to understand the Russian processes. A white paper summarizing the U.S. team's understanding of the Russian processes is available in the HSR program office. This understanding was developed during the course of several reviews of the progress of the aircraft modifications and mutual planning of the flight experiments. U.S. personnel have been to Moscow three times between August 1994 and June 1995. Russian personnel have been to the U.S. twice during the same period. The airworthiness process has been a subject of consideration at all of the international interchanges. Prior to the first TU-144 flight, another review of the aircraft modifications is scheduled for September 1995. The U.S. industry/NASA personnel (including safety and mission assurance personnel) are scheduled to attend the Russian flight readiness methodological council meeting in January 1996.

Detailed review of results from the feasibility studies, ground and system checks, aircraft modification reviews, mission planning, and the flight readiness methodological council meeting, all represent the effort that the U.S. industry/NASA team will expend toward ensuring that all design and safety data and operational characteristics of the aircraft have been fully explored. This is evidenced by the deletion of the supersonic boom experiment because of unresolved issues in flight operations, flight safety, and cost.

Finding #25:

Wind shear encounters, while infrequent, constitute a highly significant aviation hazard that has been a causal factor in major crashes. A joint NASA/Federal Aviation Administration (FAA)

Airborne Wind Shear Sensor Program has developed methods, already being implemented, for providing timely warning to aircraft in danger of encountering such atmospheric conditions.

Recommendation #25:
Continue research relating to wind shear and other aircraft-threatening phenomena, such as wake vortices, and the transfer of related technologies to users.

NASA Response to Recommendation #25:
NASA's Windshear program is now complete. The results of this successful wind-shear technology program were adopted by the avionics manufacturers for their development into safety technology for transport aircraft. One manufacturer, AlliedSignal, provided Continental Airlines, one of their customers, with their Model RDR-4D system. This is a combined weather radar and wind-shear radar. It was first flown in commercial service in December 1994. With the completion of the wind-shear program, NASA's expertise and facilities will be applied to the challenges posed by safely increasing the airport traffic capacity and especially the issues associated with wind-vortex encounters. The research consists of identifying and mathematically modeling wake vortices using computational fluid dynamics, existing empirical models and data from required wind tunnel and flight tests, developing and demonstrating a sensor to reveal the hazard to the flight crew, and validating a total system at a Center/Terminal Radar Approach Control (TRACON) Automation System (CTAS) field test site. Much of the technology and approach in this area is enabled by the previously successful development of wind-shear models and sensors.

Finding #26:
NASA has a coordinated program of tire research operating from the Langley Research and Dryden Flight Research Centers. This program has the capability to provide significant safety improvements for present and future aircraft and spacecraft.

Recommendation #26:
In addition to supporting the Space Shuttle and other research programs such as the High Speed Civil Transport, NASA should continue to emphasize and transfer lessons learned in the tire research effort to all segments of the user community.

NASA Response to Recommendation #26:
The CV-990 Landing System Research Aircraft (LSRA) project operated by Dryden Flight Research Center (DFRC) has been instrumental in defining Shuttle orbiter main gear tire performance. This program has been completed. Test results have been provided to the Society of Automotive Engineers (SAE), Boeing, Northrop, McDonnell Douglas, and Canadair. Unanimous agreement exists between Government agencies, the tire industry, and academia that this test facility is unique and supplies, in many areas, the highest fidelity in tire and landing gear testing ever achieved.

NASA is working with the FAA, Canadair, The Canadian Joint Aviation Authority, and others on winter runway friction issues in a proposed 5-year program. This program involves braking test runs with NASA's B-737, B-757, and CV-990 LSRA, together with several different ground friction measuring vehicles and parametric studies, using Langley's Aircraft Landing Dynamics Facility. Results of this program will have a direct impact on not only solving runway friction

and airport congestion problems, but also helping industry achieve improved tire designs, better chemical treatments for snow and ice, and runway surfaces that minimize adverse weather effects. Flight-crew recognition of less than acceptable reported runway friction conditions, prior to the go/no-go or the land/go around decision point, is one of the near-term goals.

Finding #27:
The Dryden Flight Research Center (DFRC) has completed a demonstration of the concept of a Propulsion Controlled Aircraft (PCA) system using an F-15 aircraft flight test and an MD-11 simulator demonstration. This system permits an aircraft to be guided to a landing in an emergency using only thrust for flight path control. DFRC is now exploring a joint program with industry to extend the demonstration to a flight test on a large commercial aircraft. Although the PCA concept has been proved, the pilot control interface aspects of the design have yet to be systematically addressed.

Recommendation #27:
Any flight test program on a large commercial aircraft should include a strong focus on selecting the optimum pilot control interface for the system.

NASA Response to Recommendation #27:
Aircraft pilot interface is critical when dealing with emergency situations. Therefore, the PCA project has conducted simulator studies that addressed the pilot interface with the PCA system. A comprehensive study in the Ames Advanced Concepts Flight Simulator looked at inputting PCA commands using modern sidestick controllers and autopilot glare shield control panel (GSCP) knobs (pitch and heading/track). Six pilots flew 100 approaches with various levels of turbulence. Pilot ratings, touchdown dispersions, and pilot opinions all showed a preference for using the GSCP knobs. The slow response of the PCA is more consistent with the autopilot response that is commanded by the GSCP controllers. It was shown that in an emergency situation, the use of sidestick controller to command the slow PCA system could result in a Pilot Induced Oscillation. The pilots will be specifically requested to address aircraft pilot interfaces during the upcoming MD-11 PCA evaluation flights.

Finding #28:
The range safety policy for Unmanned Aerial Vehicle (UAV) operations within the Edwards Air Force Base range worked when the Perseus program suffered an in-flight failure. Range safety for Perseus flights outside of the controlled airspace at Edwards has yet to be addressed.

Recommendation #28:
Consideration should now be given to establishing a UAV policy to cover Perseus flights conducted outside of controlled airspace at Edwards.

NASA Response to Recommendation #28:
The use of non-Edwards controlled airspace falls under the regulation of the FAA. The Office of Aeronautics, through the Environmental Research Aircraft and Sensor Technology (ERAST) program, has for the past 2 years been participating in workshops sponsored by the FAA for the

purpose of developing Federal Aviation Regulations needed to establish the appropriate oversight of Remotely Piloted Aircraft flight operations in the National Airspace System. Draft Advisory Circulars have been prepared and are currently undergoing legal review. The ERAST program will continue to work with the FAA toward implementing the needed regulations.

E. OTHER

Finding #29:
The Simplified Aid for EVA Rescue (SAFER) was successfully flight tested on the STS-64 mission. Although designed as a rescue device for an astronaut who becomes untethered, SAFER has demonstrated its potential to assist in other safety-critical situations such as contingency EVAs. Five SAFER flight units have been ordered. Plans are to deploy them on Mir and Space Station as well as to carry them on the Space Shuttle only when an EVA is planned.

Recommendation #29:
Once the flight units are available, NASA should consider routinely flying SAFER units on all Space Shuttle missions which do not have severe weight limitations. This will permit them to be used for those contingency EVAs in which safety can be improved
by giving crew members the capability to translate to the location of a problem to make an inspection or effect a repair.

NASA Response to Recommendation #29:
NASA has considered routinely flying SAFER units on all Space Shuttle missions which do not have severe weight limitations and has decided that it is not required.

SAFER was specifically designed to be used to rescue an EVA crewmember who had become inadvertently detached from a structure under the circumstances where the Shuttle could not credibly effect a rescue (for example, during Space Station operations when the Shuttle is either not at the Station or is docked to it). As such, it is classified as an "emergency" device and only needs to be single-string (i.e., zero-fault tolerant).

SAFER is not required for other (operational) EVA's. All known, credible, contingency EVA's can be safely accomplished without it. There currently exists an EVA method to get to the External Tank (ET) umbilical doors located on the Orbiter without SAFER, for which each EVA crewmember is briefed prior to flight.

Furthermore, the cost of making SAFER operational on all Shuttle flights would be high. To be used as other than an emergency device, significant redesign would be required to make it at least single-fault tolerant. SAFER cannot be stowed on the Primary Life Support Subsystem in the airlock; therefore, special stowage would be required on each flight. Flying two SAFER units on each flight would require stowage for about 8 cubic feet and 200 pounds. Additional EVA training would also be required each time SAFER is flown, regardless of whether or not it is planned to be used.

Given the above reasons including the fact that all known, credible, contingency EVA's can be safely accomplished without SAFER, NASA believes that implementing this recommendation is not appropriate at this time.

Finding #30:
NASA has established a Software Process Action Team (SPAT)to review and develop plans for addressing the software concerns that have been raised within NASA and by several review boards including the National Research Council and the Aerospace Safety Advisory Panel. While NASA has extensive procedures for addressing software issues in some arenas, these issues have not received uniform recognition of their importance throughout the Agency.

Recommendation #30:
NASA should ensure that computer software issues are given high priority throughout the agency and that those addressing these issues are given the support needed to produce adequate ways of dealing with them. The creation of the SPAT was an important initial step toward dealing with complex safety critical problems, but much more needs to be done.

NASA Response to Recommendation #30
NASA fully agrees with the recommendation that computer software issues must be given a high priority throughout the Agency. Recent actions taken and decisions made in the Zero-Base Review operating guidelines supports the NASA senior managers' high priority for the critical and complex software issues. NASA offered a pilot Software Program/Project Management course in March 1995. This training exhibits a priority of software issues within NASA. The follow-on "Software Acquisition" training course will be provided in August 1995 to NASA managers with significant software in their projects.

The Independent Verification and Validation (IV&V) Center of Excellence addresses complex critical software issues across NASA with the Software Improvement Initiative and IV&V on projects. The Agencywide Software Improvement program and the Agencywide Software Working Group will coordinate software issues that affect the Agency. The Software Working Group Charter gives each member the responsibility and authority to represent the software needs of their respective Center. The consolidation of IV&V projects to the NASA facility aids in addressing software issues with uniform recognition of importance across the Agency.

The Program Office representation to the Software Working Group has been strengthened. The Software Process Action Team merged with an existing working group to formulate the current Software Working Group, with cochairs from the IV&V Center of Excellence and the Chief Engineer's Office. Active Program Office support and participation in the Software Working Group would better accomplish the ASAP's Recommendation #30.

Finding #31:
There were several in-flight and ground-based episodes in which astronauts developed adverse reactions to substances used in human experiments. Although the researchers guiding these experiments submit the protocols to standard Institutional Review Board (IRB) process, there is no independent oversight of the safety of human experiments within NASA.

Recommendation #31:
NASA should provide independent oversight of human experimentation by establishing a review process in addition to the standard IRB and ensuring that the Space Shuttle and Space Station systems requirements provide sufficient equipment, staffing and training to react appropriately to any problems which might be experienced.

NASA Response to Recommendation #31:
NASA has disbanded the former Human Research Policy and Procedures Committee (HRPCC) and replaced it with an IRB. This IRB has a broader representation from operationally oriented people and physicians in addition to the researchers formerly constituting the HRPCC. Also, there is a safety representative from the JSC Office of Safety, Reliability, and Quality Assurance that participates as a member of the new IRB. NASA believes that the broader representation, combined with the continued presence of the safety representative, provides the appropriate level of safety oversight for this review process that is being sought by the ASAP. This also corrects previous shortcomings in the review process. The oversight processes of the JSC Office of Safety, Reliability, and Quality Assurance and the International Space Station Independent Assessment Panel have been designed to assure that requirements deficiencies related to equipment, staffing, and training that may exist in the Space Shuttle and Space Station programs are identified and dealt with appropriately.

Finding #32:
The number of reports submitted to the Aviation Safety Reporting System (ASRS) has nearly doubled since 1988 and has consistently been above the levels projected when the system was started. In these same years, budgetary resources have remained flat so that, even with significant productivity increases, the portion of incidents that receive detailed analysis has declined. In addition, ASRS has not been able to develop cost effective electronic dissemination of advisories or a program of educational outreach to expand use of ASRS by the aviation community, both of which would be significant safety enhancements.

Recommendation #32:
NASA and the FAA should restore the full capability of analysis, interpretation, and dissemination of the ASRS and promote electronic dissemination and expanded educational outreach.

NASA Response to Recommendation #32:
In 1993, the FAA asked the National Academy of Public Administration (NAPA) to review this program and to recommend how to improve and evolve the system. In August 1994, NAPA published their report concluding that ASRS is "a credible, resilient and worthwhile program" and cited it as a model for interagency cooperation. Recommendations from this report led to the formation of an FAA/NASA interagency team to develop an action plan that was submitted in November 1994. After several reviews, the action plan was approved. The FAA funded initial work in February 1995 and plans to fund to completion in FY 1996. This program consists of the following four major elements:

(1) An increase in effort to cover the growth in the number of reports submitted and to expand the number of "call back" validations conducted.

(2) A modernization program to improve the performance of the computer systems supporting data input and analysis. The evaluation of artificial-intelligence techniques to provide screening and sampling as well as the use of statistical techniques (These techniques should substantially reduce the work required to perform the analysis for input). A modernization program is expected to yield electronic distribution of derivative data in the form of CD/ROM and Internet distribution.

(3) Initiation of an educational and promotional program directed at members of the industrial community, as well as the FAA analysts whose work can be enhanced by access to these data. The effort will include the electronic distribution of
ASRS products including CALLBACK and DIRECTLINE.

(4) The expansion of the ASRS to solicit input from a wider range of the flight community, including cabin attendants, mechanics, and technicians.

NASA is already conducting activity to improve the ASRS including the issues raised by the findings and recommendations identified by the ASAP.

Finding #33:
For many years, NACA and NASA aeronautical research and flight safety benefitted from the advise and counsel provided by an advisory group of aircraft operations specialists consisting of representatives from civil and military aviation and manufacturers of aircraft, engines, and accessories as well as NACA/NASA personnel.

Recommendation #33:
NASA should restore the previous capacity to capture the operational experience it found useful in improving its research focus and flight safety.

NASA Response to Recommendation #33:
The Office of Aeronautics, in consultation with DFRC and others, will assess potential changes to the current Aeronautics Advisory Committee's subcommittee structure that would provide improved advice and council on aircraft safety and operating problems.

APPENDIX C

NASA AEROSPACE SAFETY ADVISORY PANEL ACTIVITIES FEBRUARY–DECEMBER 1995

FEBRUARY	
1–3	STS-63 Mission Meetings and Launch, Kennedy Space Center
7–8	Space Shuttle Mir Briefing, Johnson Space Center
MARCH	
15–17	Processing Operations Review, Kennedy Space Center
16	Testimony before the Subcommittee on Space and Aeronautics, Committee on Science, House of Representatives' hearing on "The Outside Opinion: NASA Restructuring Space Shuttle/ Space Station Reusable Launch Vehicles", Washington, DC
22	Panel Plenary Session, NASA Headquarters
23	Aerospace Safety Advisory Panel Annual Meeting, NASA Headquarters
APRIL	
11	Letter to Chairman Sensenbrenner responding to followup questions from March 16 hearing
12	Space Shuttle Program Discussions with General Accounting Office, NASA Headquarters
19–20	Review of Aeronautics and Human Factors Safety Programs, Ames Research Center
MAY	
8	Space Shuttle Downsizing Review, NASA Headquarters
9–11	Intercenter Aircraft Operations Panel Meeting, Lewis Research Center
15	Letter Report to Administrator on Panel Review of Space Shuttle Management Independent Review , NASA Federal Laboratory Review, and Zero Base Review
16	Testimony before Subcommittee on Science and Technology and Space, US Senate's hearing on "Space Shuttle and Reusable Launch Vehicle Programs"
24–25	Review of Space Shuttle Main Engine and Center Safety Programs, Marshall Space Flight Center

JUNE	
2	STS-71 Flight Readiness Review, Kennedy Space Center
13	Review of Redesign Solid Rocket Motor Program, Thiokol Corporation
14–15	Review of the External Tank Activities, Michoud Assembly Facility
21–23	STS-71 Mission Meetings and Launch, Kennedy Space Center
28	Review of Space Shuttle Main Engine Turbopump Nozzle Cracks, Rocketdyne
JULY	
10	Space Shuttle Main Engine Turbopump Nozzle Cracks Interview, Dallas
11–12	Review of Space Shuttle Main Engine Turbopump Program, Rocketdyne
13	Review of Aeronautics Safety Programs, Langley Research Center
19–20	Review of Space Shuttle and International Space Station Safety Programs, Johnson Space Center
19	Panel Plenary Session, Johnson Space Center
26	Review Meeting of GAO Report on Space Shuttle in Support of Space Station, NASA Headquarters
AUGUST	
3–4	Software Review, Johnson Space Center
9	Interview on Yellow Creek's Advanced Solid Rocket Motor Program, NASA Headquarters
10	Space Shuttle Restructuring Meeting, NASA Headquarters
31	Space Shuttle Main Engine High Pressure Fuel Turbopump Assessment Team Report to the NASA Administrator
SEPTEMBER	
22	Review of Space Shuttle Safety Operations in preparation of September 27 Testimony, Kennedy Space Center
27	Testimony before the Subcommittee on Space and Aeronautics, Committee on Science, House of Representatives' hearing on "The Space Shuttle Program in Transition: Keeping Safety Paramount"

OCTOBER

16	Panel Plenary Session, Lancaster, CA
17	Review of Aerospace Projects, Dryden Flight Research Center
18	Review of Space Shuttle Main Engine Blocks I and II Programs, Rocketdyne
18	Review of Space Station Electric Power System, Rocketdyne
19	Review of Space Shuttle Orbiter Program, Rockwell
19	Review of the Information Technology and Software, Ames Research Center
24	Letter to Chairman Sensenbrenner responding to folloup questions from September 27 hearing on "The Space Shuttle Program in Transition: Keeping Safety Paramount"

NOVEMBER

1–2	Integrated Logistics Panel Meeting, Kennedy Space Center
28–29	Panel Plenary Session, NASA Headquarters
28	Review of Safety and Mission Assurance Restructuring, NASA Headquarters
29	Review of Space Station Security Concerns, NASA Headquarters
29	Review of Space Shuttle Restructuring, NASA Headquarters

DECEMBER

14	Review of Space Shuttle Restructuring and Privatization, NASA Headquarters

National Aeronautics and
Space Administration

For Further Information Please Contact:

Aerospace Safety Advisory Panel
NASA Headquarters